Global Innovation and Strategy Center

The Characterization and Measurement of Cyber Warfare

Spring 2008 – Project 08-01
May 2008

Intern Researchers:
Kyle Dobitz
Brad Haas
Michael Holtje
Amanda Jokerst
Geoff Ochsner
Stephanie Silva

Project Management and Oversight:
1Lt Kevin Johnson
John G. Hudson II

Approved: Kevin E. Williams, SES, DAF
Director, Global Innovation and Strategy Center

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
MAY 2008	FINAL REPORT	FEBRUARY 2008 - MAY 2008

4. TITLE AND SUBTITLE

The Characterization and Measurement of Cyber Warfare

5a. CONTRACT NUMBER

N/A

5b. GRANT NUMBER

N/A

5c. PROGRAM ELEMENT NUMBER

N/A

6. AUTHOR(S)

Dobitz, Kyle
Haas, Brad
Holtje, Michael
Jokerst, Amanda
Ochsner, Geoff
Silva, Stephanie

5d. PROJECT NUMBER

08-01

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

USSTRATCOM Global Innovation and Strategy Center (GISC)
Intern Program
6805 Pine Street
Omaha, NE 68106

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

USSTRATCOM Global Innovation and Strategy Center (GISC)
6805 Pine Street
Omaha, NE 68106

10. SPONSOR/MONITOR'S ACRONYM(S)

USSTRATCOM - GISC

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Hostile exercises across computer networks are today increasingly common, and the proliferation of such activity is a national security concern. The characterization of cyberspace activity is the subject of much debate; the unique nature of the cyber arena calls into question traditional state boundaries and operational codes of conduct. Actors in cyberspace can exhibit influence from anywhere in the world, thus many hostile acts are difficult to trace. Additionally, targets in cyberspace are often intangible, rendering an appropriate response that is difficult to discern. This report provides a framework useful for delineating such acts, utilizing existing literature and current international law as a frame. Additionally, this research utilized the assumption that all actors and actions in cyberspace carry inherent risks, and did not separate “bad” actions from “good.”The following factors were identified by the research team as critical for purposes of cyber act characterization: Motivation, Intent, Target, Effects, and Actors.

15. SUBJECT TERMS

cyberspace, cyber warfare, targets, motivation, intent, effects, actors, cyber legal, characterizing cyber acts

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. John G. Hudson II
U	U	U	UU	88	19b. TELEPHONE NUMBER *(Include area code)* 402-398-8034

The Characterization and Measurement of Cyber Warfare

Preface

This report is the product of the Global Innovation and Strategy Center's (GISC) Internship program. This program is constructed of combined teams of six graduate and undergraduate students, with the goal of providing a multidisciplinary, unclassified, non-military perspective on important Department of Defense issues.

The Spring 2008 team, composed of students from the University of Nebraska at Omaha and the University of Nebraska at Lincoln, was charged with undertaking the problems associated with characterizing actions in cyberspace. Hostile computer operations lack clear taxonomies across both domestic policy and international law, and that deficiency directly impacts incident assessment and decision making.

This project took place between February and early May 2008, with each team member working twelve to twenty hours per week. While the GISC provided the resources and technology for the project, it was solely up to the team to develop the project design, conduct the research and analysis, and provide appropriate recommendations.

Acronyms

CIA	Central Intelligence Agency
CIP	Critical Infrastructure Protection
CNA	Computer Network Attack
CNAE	Computer Network Attack and Exploitation
CND	Computer Network Defense
CWIN	Critical infrastructure Warning Information Network
DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DOD	Department of Defense
DOS	Denial of Service
FERC	Federal Energy Regulation Commission
FISMA	Federal Information Security Management Act
GAO	General Accountability Office
HTTP	Hypertext Transfer Protocol
IA	Information Assurance
IATAC	Information Assurance Technology Analysis Center
ICJ	International Court of Justice
IHL	International Humanitarian Law
ISAC	Information Sharing and Analysis Center
ICJ	International Court of Justice
ISP	Internet Service Provider
IT	Information Technology
NSCD	National Security Cyber Division (DHS)
NSPD	National Security Presidential Directive
NIEX	No-notice Interoperability Exercises
JWICS	Joint Worldwide Intelligence Communications System
NIPRNET	Nonsecure Internet Protocol Router Network
NSA	National Security Agency
TCP/IP	Transmission Control Protocol/Internet Protocol
SIPRNET	Secret Internet Protocol Router Network
SSL	Secure Sockets Layer
JWICS	Joint Worldwide Intelligence Communications System
UN	United Nations
USAPATRIOT	Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism Act of 2001
US-CERT	United States Computer Emergency Readiness Team
USC	United States Code
USSTRATCOM	United States Strategic Command

Executive Summary

Hostile exercises across computer networks are today increasingly common, and the proliferation of such activity is a national security concern. The characterization of cyberspace activity is the subject of much debate; the unique nature of the cyber arena calls into question traditional state boundaries and operational codes of conduct. Actors in cyberspace can exhibit influence from anywhere in the world, thus many hostile acts are difficult to trace. Additionally, targets in cyberspace are often intangible, rendering an appropriate response difficult to discern. This report provides a framework useful for delineating such acts, utilizing existing literature and current international law as a frame. Additionally, this research utilized the assumption that all actors and actions in cyberspace carry inherent risks, and did not separate "bad" actions from "good."

The following factors were identified by the research team as critical for purposes of cyber act characterization:

- Motivation – Cyber actors can have one or more motivations underlying their activity. Cyber actors might be motivated to act out of personal interest, ideological interest, political interest, national interest, or no particular interest at all. Moreover, the motivations of cyber actors differ from one another in terms of the degree of malice.

- Intent – Intent refers to the primary objective of the cyber actor, or what the actor is hoping to accomplish. Intent is judged against how permissible or prohibited an action is.

- Target – Targets range from non-protected, non-critical units to highly protected, classified, critical systems or infrastructure. The target is critical to assessing not only the level of intrusion an act represents, but also the level of potential harm an uncontrolled attack could cause.

- Effects - Effects are an extremely significant factor for act characterization and the primary argument for international cooperation. Effects can be measured by financial damage, physical damage or the level of human harm resulting from a cyber act.

- Actors – Attack origination is key to assessing appropriate response priorities. However, actor(s) identification is not needed to assess the typology of the act initially.

Providing a nascent nomenclature, the combination of these four factors will assist in discerning events; when juxtaposed with decision-making metrics, such a blueprint can enhance incident comprehension. Furthermore, the flexibility of the framework allows evolution with use, clarifying operational and budgetary needs. Long-term refinement will also elucidate statutory means necessary for agile cyberspace management.

Cyber Warfare Overview

> Mastery of cyberspace is essential to America's national security. Controlling cyberspace is the prerequisite to effective operations across all strategic and operational domains—securing freedom from attack and freedom to attack.[1]
>
> - 2007 Air Force Cyber Command Strategic Vision

Over the last three decades, organizations of every kind – government, military, commercial, and private – have developed a pervasive and enduring reliance on both the public Internet and networked systems overall. Thus far, the general approach has been to adopt new technologies as soon as they became available, with little or no consideration for the possibility of their misuse. Since global dependence on the Internet and malicious use of it have both reached high levels and continue to grow, the need for government institutions and public policy concerning cyber security has become critical.

Twenty-five years after its creation, many entities implicitly trust the Internet, yet there is no control over who can join it and potentially abuse it. Internet-connected systems are regularly probed by entities ranging from automated malware seeking new victims to expert hackers executing precise, sophisticated attacks. Users run software that almost always contains vulnerabilities, on hardware that is not guaranteed to be trustworthy, using an Internet designed with reliability and performance – not security – in mind. Moreover, terrorists and other hostile parties are developing methods to exploit these vulnerabilities, while simultaneously growing more dependent on cyberspace themselves. Therefore, the United States government must rise to

[1] Air Force Cyber Command Strategic Vision. Comments by Major General William T. Lord. (n.d.).

the challenge of establishing dominance in cyberspace, protecting American interests, and preparing for cyber operations against enemies.

History of Cyberspace

Misuse

Even before computers and networks could be used for substantial legal or criminal gain, problems arose in shared systems. Both intentionally and unintentionally, users were able to make shared systems behave in ways not expected by the system designer. For example, users could acquire extra time on the system or access memory in another user's domain. These problems led system designers to implement protection in primitive operating systems, and those protection methods are still in use today. However, early users found other ways to circumvent the boundaries imposed by the system, which in turn led to more changes imposed by system designers.[2] This was the beginning of an ever-escalating conflict between software designers and users. Not until recently have designers begun to be wary enough of the general public to create more secure software.

In the 1972 *Computer Security Technology Planning Study*, James P. Anderson wrote that design flaws, and the fact that systems were not designed to be secure, "provide a malicious user with any number of opportunities to subvert the operating system itself."[3] The study called for systems to be securely designed with three requirements: adequate system access control, authorization mechanisms, and controlled execution of any programs being executed on a user's behalf. Little has changed since that 1972 article, especially regarding the third requirement. The

[2] Pfleeger, Charles P. and Shari Lawrence Pfleeger. Security In Computing, 3rd Edition. Upper Saddle River, NJ: Prentice Hall, 2003.
[3] Anderson, James P. Computer Security Technology Planning Study, Volume II. USAF Electronic Systems Division, Command and Management Systems, 1972.

buffer overflow, which enables an attacker to gain complete control over a program, has been the basis of the most significant computer exploits of the last three decades.

History of the Internet

At its inception, the Internet showed no signs of the size and ubiquity it experiences today. Originally, it was a project of the Defense Department's Advanced Research Project Agency (DARPA) designed to ease communication among researchers.[4] In 1969, four universities were connected. During the following decade dozens more joined. The development of the Transmission Control Protocol / Internet Protocol (TCP/IP) standard occurred in 1983.[5] These protocols remain the foundation of the current Internet.

During the next two decades, the US military developed separate networks, which would eventually become the Nonsecure Internet Protocol Router Network (NIPRNET), the Secure Internet Protocol Network (SIPRNET), and the Joint Worldwide Intelligence Communications System (JWICS).[6] As the military developed these networks, the commercial Internet continued to grow. The development of the Hypertext Transfer Protocol (HTTP) and the World Wide Web gave rise to the e-commerce boom of the late 1990s. The increasing sophistication of all types of devices and wireless technologies further contributed to the development of the Internet of today.

This rapid development was accompanied by rapid adoption. The appeal and utility of Internet-connected systems exceeded concern for prudence and caution. As more organizations became connected, network vulnerabilities multiplied. Savvy, opportunistic hackers began to identify and attack vulnerabilities in computers, networks, and related systems. As administrators attempted to catch up, the field of Information Assurance (IA) gained momentum.

[4] Grant, Rebecca. "Special Report: Victory In Cyberspace." Air Force Association Special Report, October 2007.
[5] Ibid.
[6] Ibid.

Computer Attacks and Defenses

Traditionally, computer security measures are based on the protection of three fundamental attributes: confidentiality, integrity, and availability. Nearly all cyber attacks seek to compromise at least one of these three attributes. Confidentiality and integrity both relate to data. Confidentiality refers to a restriction on the reading of data to allow access only to authorized parties. Similarly, integrity restricts modification of data to authorized parties. The third attribute, availability, refers to the availability of the system to users. A breach in availability is commonly called a Denial-of-Service (DOS) attack.

Computer attacks typically exploit a system or network in an unexpected manner, enabling the attacker unauthorized access or control. However, a breach in security does not necessarily require sophisticated techniques. Attacks can be logical, as in the case of software vulnerability exploitation, or physical, as in the destruction of a network link. They may also involve manipulating people, via "social engineering,"[7] into volunteering information or access. Attacks can be local, requiring the attacker to have some prior access to the system, or remote, carried out from afar through the Internet. They can make use of only the attacker's own resources, or they can use other compromised systems using "bots"[8] to carry out the attack. The attacker may gain partial control over a system, or total control, known as "root access."[9]

[7] Social engineering is a method used by malicious actors to gain computer passwords or other access information they would not normally be privy to, via socially accepted methods of communication. For example, the actor may falsely represent themselves as a bank official or technical support representative with a supposedly legitimate need for such access tools.

[8] A "bot" refers to the infection of a computer with remote-controlled software to enable a third party access for illicit purposes. See: "FBI Unveils Movable Feast with 'Operation Bot Roast,'" by Brian Krebs in the June 13, 2007 edition of *The Washington Post* for an overview.

[9] "Root access" refers to administrative level computer or network access, to the core of the computer or network.

As cyber attacks and defenses developed, various threats rose and fell. The popular targets sought by cyber attackers have shifted from systems (such as Microsoft® Windows™ platforms) to the applications running on those systems (such as web server programs). The goals of hostile cyber actors have also changed; where publicity may have previously been the prime motivator, profit serves as the motivation of many actions today. An enormous underground market has emerged for illegally obtained data and access. Methodology has changed as well. The most dangerous acts are not overt, but instead quietly persist and collect information for use in espionage, fraud, and other illegal activities.

Current Threats

A 2006 study reported that nearly all terrorist groups operate web sites and use their technical skills "for communications, fundraising, propaganda, recruitment, target reconnaissance, and training."[10] The FBI has corroborated this assessment, citing uses of fraud to support Al Qaeda and other terrorist activities.[11]

Other computer criminals also pose threats to US infrastructure, either independently or as accomplices to terrorists plotting larger operations. Insiders also pose a risk; according to a 2007 report by the Department of Homeland Security (DHS), "Individuals such as contractors, employees, and service providers who have legitimate access to critical computer systems often have detailed operational and security knowledge and physical access that would facilitate a cyber attack."[12] These threats are compounded by widespread use of commonly available

[10] Westby, Jody. Countering Terrorism with Cyber Security. Paper for the 36th Session World Federation of Scientists, International Seminars on Planetary Emergencies, Erice, Italy, August 18-26, 2006.
[11] Rollins, John, and Clay Wilson. Terrorist Capabilities for Cyberattack: Overview and Policy Issues. Congressional Research Service Report for Congress, 22 January 2007.
[12] United States. Office of Intelligence and Analysis for Homeland Security. Homeland Security Assessment. 5 June 2007.

protocols and products, as well as heavy interconnection among all types of organizations. The private sector, in particular, has grown heavily dependent on the public Internet, with consumers demanding perpetual account access and information, resulting in an economic vulnerability for the US economy. This has led to the creation of such self-protecting information sharing organizations as the Information-Technology Information Sharing and Analysis Center (IT-ISAC).[13]

Indeed, the US economy itself, or segments of it, is an enormous national security interest, in many ways akin to actual physical targets. A cyber action intended to overwhelm western markets might prove catastrophic to the national or international economy; such a situation could also have traumatic psychological effects on the general population that might represent the hostile cyber actor's true goal.[14] Additionally, while national security resources are an obvious and tantalizing mark for hostile cyber actors, their mere connection to the public Internet increases exposure. The 2001 Internet worm Code Red is a prime example, infecting over 250,000 systems in nine hours:[15]

> As a result of the attacks, DOD was forced to shut down its Web sites; the White House was forced to change its Internet address; the Department of the Treasury Financial Management System was infected and had to be disconnected from the Web…the Federal Express package-tracking system was infected, causing delivery delays.[16]

Initial economic damages were projected at $2.4 billion; final dollar amounts are not publicly available.[17] [18]

---

[13] Information Technology – Information Sharing and Analysis Center (IT-ISAC): "Frequently Asked Questions," 2006. Accessed via the world wide web April 2008. <https://www.it-isac.org/faq.php>
[14] Rochte, Russell C. Roundtable discussion, Washington D.C. 14 May 2008.
[15] Binnendijk, Hans, ed. Transforming America's Military. National Defense University Center for Technology and National Security Policy, National Defense University Press, 2002.
[16] Ibid.
[17] Ibid.
[18] Arquilla, John. E-mail to Stephanie D. Silva. 10 July 2008.

Current Trends

While past hostile cyber actions were perhaps more blatant and high-profile, the current trend appears to be a stealth amassing of thousands of compromised computers for use in further attacks or to steal financial data. For example, a seven-month study in 2006 revealed 100,490 credit cards and other financial accounts being traded in one Internet black market group.[19] The estimated wealth generated from this illicit activity was over $93 million.[20] Additionally, malware techniques (allowing attackers to avoid detection entirely as they gain control of computers) are becoming increasingly sophisticated. Compromised computers, or "bots," enable attackers to perform massive reconnaissance and DOS attacks. The threat to US interests is growing. Unauthorized parties attempt to access U.S. military computer networks over three million times a day, much more frequently than those of other countries.[21] Additionally, there is increasing cooperation among illicit cyber actors, organized crime, and terrorists.[22]

American organizations and individuals share the same need to guarantee the confidentiality, integrity, and availability of computer systems and networks. According to a 2007 Congressional research report, "DOD officials have noted that because 80 percent of US commerce goes through the Internet, DOD systems must develop a capability to adequately

19 Franklin, Jason, et al. "An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants." Conference on Computer and Communications Security, Alexandria, Virginia October 29 – November 2, 2007.
[20] Ibid.
[21] Wilson, Clay. Emerging Terrorist Capabilities for Cyber Conflict Against the US Homeland. Congressional Research Service, 1 November 2005.
[22] Wilson, Clay. Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. Congressional Research Report Service for Congress, 29 January 2008.

protect [the Internet]."[23] A 2005 *Naval Law Review* article reported that an estimated "95% of military information traffic utilizes civilian networks at some stage of the communication."[24] The Defense Technical Information Center's Information Assurance Technology Analysis Center (IATAC) states:

> (The US) is vulnerable to Information Warfare attacks because our economic, social, military, and commercial infrastructures demand timely and accurate as well as reliable information services. This vulnerability is complicated by the dependence of our Department of Defense (DOD) information systems on commercial or proprietary networks which are readily accessed by both users and adversaries."[25]

This necessity of defense, coupled with enemies' growing dependence on information technology, drives DOD interests in the domain of cyberspace. The DOD defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." [26]

In addition to DOD interests, cyber warfare capabilities must also be formed in scope and magnitude by foreign policy and international law. Currently, the US and the international community share very few explicit, established agreements governing cyber warfare and cyber crime. Therefore, when cyber conflicts arise, it is unclear how America's adversaries and allies will proceed. The following history of cyber conflicts illustrates this lack of clarity.

---

[23] Wilson, Clay. Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Issues. Congressional Research Service Report for Congress, 20 March 2007.
[24] Antolin-Jenkins, Vida. "Defining the parameters of cyberwar operations: looking for law in all the wrong places." Naval Law Review, 51:132. (2005).
[25]" Information Assurance Technology Analysis Center: History." (n.d.). <http://iac.dtic.mil/iatac/history.html>.
[26] U.S. Department of Defense, Memorandum from the Office of the Secretary of Defense, definition of Cyberspace, May 12, 2008.

Eligible Receiver (1997)

Eligible Receiver is a cyber exercise sponsored by the Chairman of the Joint Chiefs of Staff, and is a No-Notice Interoperability Exercise (NIEX), designed to test operational readiness in the event of a crisis.[27] Exercises are generally regional – not global – and little notice, if any, is given to departments and agencies responsible for responding.[28] Though the first Eligible Receiver exercise took place in 1987,[29] a well-documented exercise year is 1997, when the National Security Agency successfully accessed classified Pentagon systems, taking control of Pacific Command networks.[30]

Moonlight Maze (1999)

In 1999, cyber actors of unknown origin performed a series of cyber attacks against US military systems and successfully intercepted data. The attacks, termed "Moonlight Maze," targeted classified information on naval codes and missile guidance systems.[31] Though Russian involvement was suspected, the original perpetrator remains unknown. PBS interviewed noted cyber expert Dr. John Arquilla on the event, who stated, "Had the data in question that was being pilfered been strongly encrypted, it would have been of no use to the intruders. But the fact of the matter is most of the material taken was cued up at a printer where it's, first of all, not behind a secure firewall, and secondly, not at all encrypted…it was simply plucked."[32]

---

[27] Joint Chiefs of Staff. "No-notice Interoperability Exercise Program." Chairman of the Joint Chiefs of Staff Instruction, 3510.01D, 21 March 2008.
[28] Ibid.
[29] "Eligible Receiver." Defense Technical Information Center, powerpoint. Accessed world wide web April 2008. <www.dtic.mil/doctrine/training/wjtsc07_2wg_exsynch_er.ppt>
[30] "CyberWar!" PBS Frontline, 24 April 2003.
[31] Cabana, Nonie. "Cyber Attack Response: The Military in a Support Role." Air & Space Power Journal, April 4 2008 <http://www.airpower.maxwell.af.mil/airchronicles/cc/cabana.html>.
[32] CyberWar!" PBS Frontline, 24 April 2003.

China – US (2001)

When a US reconnaissance aircraft collided with a Chinese fighter jet in 2001, Chinese hackers mounted an attack against the U.S. As in the Palestine-Israel conflict, attackers distributed programs to increase the attack's magnitude and coordination. When China was slow to release the crew of the American aircraft, U.S. hackers launched their own program against Chinese entities. The coordinating groups on both sides eventually declared a truce, but only after each (allegedly) defaced approximately one-thousand websites.[33]

Palestinian – Israeli Cyberwar (2003)

A 2003 Army report details the Palestinian-Israeli cyber conflict that took place between 1999 and 2001. The conflict began when Israeli teenagers conducted a DOS (Denial of Service) attack against Hezbollah and Hamas websites. Palestinian hackers and supporters responded by attacking websites belonging to Israeli government and commercial organizations. The attackers published tools, which volunteers could obtain and use to participate in the efforts without the benefit of technical skills. By January 2001, Palestinian hackers defaced 548 websites in the Israeli domain. Commercial entities and Internet providers suffered days of outages. Some American entities suffered from the conflict as well. For example, AT&T experienced attacks as they attempted to provide extra bandwidth to the attack victims.[34]

[33] Allen, Patrick D and Chris Demchak. "The Palestinian-Israeli Cyberwar." Military Review. March-April 2003.
[34] Ibid.

Titan Rain (2005)

A Congressional Research Service Report for Congress provides an overview of "Titan Rain," the name given to a series of efficient, sophisticated attacks beginning in 2003.[35] The attacks penetrated DOD systems at dozens of locations, gaining control of the systems and stealing data that, while unclassified, was sensitive. Further investigation into the attacks has been classified. Other sources[36] report that a network security analyst at Sandia National Labs traced the attacks to China. When the analyst presented his findings to his superiors, he was told to stop investigating the attacks and not to share the information with anyone. Unlike other attacks of this time frame, the attacks of "Titan Rain" were highly coordinated and very sophisticated, possibly indicating state support.

Estonia (2007)

In April of 2007, Estonia suffered perhaps the most widely publicized cyber attack to-date. In response to the Estonian government's decision to move a statue commemorating a Russian soldier, a massive DOS attack began. The attack, lasting several weeks, flooded Estonian networks and servers, disabling many of them. The attack targeted web sites of government agencies, newspapers, banks, and other organizations, which were either rendered useless or forced to shut down.[37] The US and NATO dispatched computer emergency response teams to assist. At the time, Estonia accused the Russian government of initiating the attack, but later investigation suggested that independent groups were responsible. Sources of the attack

[35] Rollins, John, and Clay Wilson. Terrorist Capabilities for Cyberattack: Overview and Policy Issues. Congressional Research Service Report for Congress, 22 January 2007.
[36] Thornburgh, Nathan. "The Invasion of the Chinese Cyberspies." Time, 29 August 2005. <http://www.time.com/time/printout/0,8816,1098961,00.html>.
[37] Grant, Rebecca. "Special Report: Victory In Cyberspace." Air Force Association Special Report, October 2007.

have been traced to systems worldwide. One man, a Russian expatriate living in Estonia, has been tried and convicted for participating in the attack.[38]

Incident Assessment

Eligible Receiver, designed specifically to measure U.S. cyber operational readiness, may showcase its only weaknesss by the very acknowledgement of its existence. Such a luxury is nonexistent during events like Moonlight Maze, which themselves reinforce the ideal of Eligible Receiver. Neither of these exercises represent the broad technological and social risks that the cyber world introduces, however, due to both rapidly changing tools and their effects outside of government networks. For example, the 2001 incident between Chinese and American hackers highlighted the fact that non-official actors can today become major players during foreign policy evets. Two years later, the Palestinian-Israel occurrence showcased a similar spillover, as ethnic tensions exploded across the cyber terrain.

Additionally, the movement of physical or territorial altercations to the cyber world can impact much more than finances or psyches; the suspected state support behind the recent Titan Rain and Estonia incidents point toward the possibility of incident transfer *back* to the physical realm – what would the United States do if its entire infrastructure was shut down for weeks on end? A variety of military and civilian forces might be a dire necessity in such an instance.

Each of these incidents reinforces the United States' need for clearer policies and procedures for dealing with cyber conflicts. A flexible, universal method of classifying such events is clearly needed. A few scholars have proffered frameworks attempting to address this

[38] Wilson, Clay. Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. Congressional Research Report Service for Congress, 29 January 2008.

problem, but those analytical tools do not by themselves produce adequate characterizations on which military officers and policymakers can base appropriate responses.

Cyber Legal Considerations

International Law Overview

There are two sources of international law: formal international agreements, such as treaties, and customary international law. Customary international law emanates from an interpretation of treaties, declarations of international bodies, statements and actions of governments, and manifestations of accepted traditional international practice.[39] [40] Treaties are only binding on parties to them; states interested in establishing new rules can initiate new treaties.[41]

Generally, international law is established by agreement among the parties who will be bound by it.[42] States who disagree with aspects of customary international law can "persistently object" during the development of those aspects, and those states are not legally bound by those aspects. State-consent, or lack thereof, leads to the general rule that if international law does not specifically prohibit an act, it tacitly permits that act.[43]

State Sovereignty

[39] Ellis, Bryan W. "The International Legal Implications and Limitations of Information Warfare: What Are Our Options?" US Army War College Strategy Research Project, 10 April 2001.
[40] Heaton, J. Ricou. "Civilians at War: Reexamining the Status of Civilians Accompanying the Armed Forces." Air Force Law Review, 57 (2005).
[41] Heaton, J. Ricou. "Civilians at War: Reexamining the Status of Civilians Accompanying the Armed Forces." Air Force Law Review, 57 (2005).
[42] Ellis, Bryan W. "The International Legal Implications and Limitations of Information Warfare: What Are Our Options?" US Army War College Strategy Research Project, 10 April 2001.
[43] Ibid.

Under the traditional understanding of sovereignty, nation-states occupy a territorially-defined physical locus, such that "sovereignty" and "country" are inextricably intertwined.[44] Nation-states are defined by the territory they control, and nation-states possess exclusive authority over events within their borders.[45]

Article 2(4) of the United Nations Charter prohibits the use of force by states against the territorial integrity and political independence of other States and codifies the legal sanctity of states' territorial borders.[46] Likewise, the UN Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States ("Non-Intervention Treaty") prohibits direct or indirect intervention in the "internal or external affairs of any state" and provides that "armed intervention and all other forms of interference … against a State … are condemned."[47] However, computer-mediated communication undermines the traditional assumption that sovereignty and territory are indistinguishable.[48]

The availability of computer-mediated communication makes physical territory increasingly irrelevant.[49] Electronic signals can travel across international borders and transit international networks with impunity.[50] Individuals or groups can affect systems around the globe, while national legal authority applies only within national borders.[51] Such intangible

[44] Walker, Jeffrey K. "The demise of the nation-state, the dawn of new paradigm warfare, and a future for the profession of arms." Air Force Law Review, 51: (Spring 2001).
[45] Ibid.
[46] UN Charter, Article 2(4). <http://www.un.org/aboutun/charter/index.html.>
[47] UN Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States. <http://www.un.org/documents/ga/res/36/a36r103.htm.>
[48] UN Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States. <http://www.un.org/documents/ga/res/36/a36r103.htm.>
[49] Brenner, Susan W. "At Light Speed: Attribution and Response to Cyber Crime/Terrorism/Warfare." The Journal of Criminal Law and Criminology , 97:2 (2007).
[50] Ibid
[51] Ibid

violations of national borders may not constitute the type of violation traditionally understood to be violative of national sovereignty.[52]

With this in mind, two options for understanding the role of national sovereignty in the realm of cyberspace exist. Under the first option, nations can attempt to impose traditional notions of territorial sovereignty onto the realm of cyberspace. Under the second option, nations can recognize how the unique attributes of cyberspace necessitate an alternative regime, perhaps leading to a conclusion that there is no national sovereignty in cyberspace.[53] Either path will require regional or global consensus, and the current nascence of cyberspace communication may prevent such dialogue today. In the coming decades, however, such legal agreements may prove inevitable; the expanded utilization of cyberspace and its associated applications will draw heavily upon the law and ask questions that render inaction impossible.

Use of Force

There is further legal ambiguity concerning the international implications of cyber warfare. Depending on their precise nature, some hostile cyber acts may constitute "uses of force" and/or "armed attacks" under international law, while other types of hostile cyber acts cannot be characterized as such. The lack of clarity exists because cyber actions do not fall seamlessly within the general legal criteria governing use of force.

No provision of international law explicitly prohibits cyber warfare, nor is there any existing authoritative legal or international agreement explicitly governing whether a cyber

[52] Ellis, Bryan W. "The International Legal Implications and Limitations of Information Warfare: What Are Our Options?" US Army War College Strategy Research Project, 10 April 2001.
[53] The Outer Space Treaty provides an existing analogy to this second option. (Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies. 18 UST 2410, 1967).

attack is comparable to an "armed attack" or "use of force."[54] Also, there is currently no accepted standard of proof for a cyber attack.[55] Such definitional ambiguity allows states or countries to engage in cyber attacks without significant legal repercussions and limits the ability of victim states or countries to identify legally-appropriate responses.[56]

Jus ad Bellum - "The Law in Waging War"

The conventional international legal regime governing the use of force by a state is the United Nations Charter. Article 2, Section 4, provides a general prohibition against the use of force by stating that nations shall "refrain … from the threat or use of force against the territorial integrity or political independence of any state…."[57] There are, however, two notable exceptions to that prohibition.

First, the UN Charter grants power to the UN Security Council to authorize force if it deems necessary. Chapter VII states that the Council may "determine the existence of any threat to the peace, breach of the peace or act of aggression;"[58] Article 42 authorizes the Council to "take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security."[59] Secondly, every member state enjoys "an inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations," as codified in Article 51.[60] Thus, unless authorized by the UN Security Council, a state may only legally employ the use of force when asserting a claim of self-defense.[61]

---

[54] Ellis, Bryan W. "The International Legal Implications and Limitations of Information Warfare: What Are Our Options?" US Army War College Strategy Research Project, 10 April 2001.
[55] Ibid.
[56] Ibid.
[57] UN Charter, Article 2(4). <http://www.un.org/aboutun/charter/index.html.>
[58] UN Charter, Chapter VII. <http://www.un.org/aboutun/charter/index.html.>
[59] UN Charter, Article 42. <http://www.un.org/aboutun/charter/index.html.>
[60] UN Charter, Article 51. <http://www.un.org/aboutun/charter/index.html.>
[61] Fidler, David P. "The International Legal Implications of 'Non-Lethal Weapons.'" Michigan Journal of International Law, 21:51 (1999).

However, a state need not wait until it absorbs an enemy's attack before claiming self-defense. The Caroline doctrine, articulated in 1842 by then-Secretary of State Daniel Webster, permits nations to engage in anticipatory self-defense when "necessity of that self-defense is instant, overwhelming, and leaving no choice of means and no moment for deliberation."[62] Additionally, after an attack occurs and is repelled, states need not wait at their borders for another attack to take place. Instead, states are permitted to continue on the offensive in order to ensure that future attacks do not occur.[63]

Despite the near-universal acceptance of the legal paradigm governing use of force by a state, there is no international consensus regarding terms that describe such. In Nicaragua *v.* United States, the International Court of Justice (ICJ) held that there are legal distinctions between: (1) an armed attack, (2) a use of force, and (3) an intervention, and the Court declared that armed attacks are the only events that trigger the right of self-defense.[64] However, no modern international legal institution has defined "act of war," "use of force," or "armed attack."[65] A similar problem arises regarding the "Non-Intervention Treaty,"[66] which prohibits direct or indirect intervention in the "internal or external affairs of any state" and provides that "armed intervention and all other forms of interference … against a State … are condemned."[67] The treaty does not define "armed intervention" nor "other forms of interference."[68]

---

[62] Kearly, Timothy. "Raising the Caroline." Wisconsin International Law Journal,17.2 (2007).
[63] O'Connell, Mary Ellen. "Enforcing the Prohibition on the Use of Force: The UN's Response to Iraq's Invasion of Kuwait." Southern Illinois University Law Journal, 15: 453 (1991).
[64] Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. US), 1986 I.C.J. 14
[65] Ellis, Bryan W. "The International Legal Implications and Limitations of Information Warfare: What Are Our Options?" US Army War College Strategy Research Project, 10 April 2001.
[66] UN Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States. < http://www.un.org/documents/ga/res/36/a36r103.htm.>
[67] UN Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States. <http://www.un.org/documents/ga/res/36/a36r103.htm.>
[68] Ellis, Bryan W. "The International Legal Implications and Limitations of Information Warfare: What Are Our Options?" US Army War College Strategy Research Project, 10 April 2001.

This failure presents both theoretical and practical problems for cyber warfare. It is unclear whether a cyber attack constitutes an "armed attack," "use of force," or "intervention." Also, it is unclear whether the legal terms refer to the *act* or the *result* of the act.[69] Even if cyber attacks produce physical effects, the attack itself is still a non-physical act perpetrated via an electronic medium.[70] Furthermore, it is unclear whether the UN-defined inherent right to self-defense includes a military response against a state conducting cyber attacks.[71]

The US tends to advocate that "reprisals involving the use of force are illegal."[72] Similarly, the 1974 UN General Assembly Definition of Aggression Resolution, which was intended to provide "useful guidance," emphasizes the role of actual or "kinetic" force.[73] Thus, cyber attacks may only constitute an "intervention" or "use of force," rather than an "armed attack," disenthralling the victim of the right to employ use of force in self-defense.[74] However, the US further "recognizes that patterns of attack or infiltration can rise to the level of an 'armed attack,'" which would justify the use of force in self-defense.[75]

Jus in Bello – "Justice in War"

Because cyber attacks may be construed as a "use of force" or "armed attack," it is necessary to consider the pertinent international law that would govern cyber attack implementation. Protocol I of the Geneva Convention requires that:

---

[69] Ibid.
[70] Ibid.
[71] Ibid.
[72] Ibid.
[73] United Nations General Assembly, Definition of Aggression Resolution 3314 (XXIV). <http://www.jstor.org/stable/view/2200318?seq=1.>
[74] Fidler, David P. "The International Legal Implications of 'Non-Lethal Weapons.'" Michigan Journal of International Law, 21:51 (1999).
[75] Ellis, Bryan W. "The International Legal Implications and Limitations of Information Warfare: What Are Our Options?" US Army War College Strategy Research Project, 10 April 2001.

> (I)n the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.[76]

Similarly, International Humanitarian Law (IHL) regulates how force and weapons may be used during armed conflict.[77] Even when legally entitled to employ the use of force, states may not do so indiscriminately.[78] States must comply with the three underlying principles of the law of armed conflict, as well as respect the status of neutral states.[79]

Necessity holds that a state may only use force when the state faces an immediate and serious threat.[80] Civilians and civilian property that make a direct contribution to the war effort may be targeted, but civilian systems that have no direct contribution may not be deliberately attacked.[81] Proportionality requires states to balance the military advantage of an attack against likely civilian harm and to use the method of attack that will cause the least amount of collateral damage.[82] Distinction requires states to distinguish civilians and civilian objects from military personnel and military objects.[83] In addition to the three principles, uses of force must also respect the sovereignty and neutrality of states not party to the conflict.[84] The nature of cyber

[76] Fidler, David P. "The International Legal Implications of 'Non-Lethal Weapons.'" Michigan Journal of International Law, 21:51 (1999).
[77] Ibid.
[78] Ibid.
[79] Heaton, J. Ricou. "Civilians at War: Reexamining the Status of Civilians Accompanying the Armed Forces." Air Force Law Review, 57 (2005).
[80] Ibid.
[81] Ellis, Bryan W. "The International Legal Implications and Limitations of Information Warfare: What Are Our Options?" US Army War College Strategy Research Project, 10 April 2001.
[82] Heaton, J. Ricou. "Civilians at War: Reexamining the Status of Civilians Accompanying the Armed Forces." Air Force Law Review, 57 (2005).
[83] Heaton, J. Ricou. "Civilians at War: Reexamining the Status of Civilians Accompanying the Armed Forces." Air Force Law Review, 57 (2005).
[84] Ellis, Bryan W. "The International Legal Implications and Limitations of Information Warfare: What Are Our Options?" US Army War College Strategy Research Project, 10 April 2001.

warfare poses problems to the traditional understanding of the necessity, proportionality, and distinction requirements, as well as the requirements concerning neutral states.

If cyber attacks do not constitute a "use of force" or "armed attack," cyber attackers need not be concerned with the requirements of necessity, proportionality, and distinction. If, alternatively, cyber attacks do constitute a "use of force" or "armed attack," it is not clear how the above-mentioned requirements apply to such attacks. The problems in applying these requirements to cyber warfare result from two general implications: first, minimizing collateral damage becomes extremely difficult,[85] and second, the intangible damage caused by information attacks is fundamentally different than the physical damage caused by traditional warfare.[86]Additionally, adherence to the distinction principle might be the most inhibited because of the dual-use nature of information systems and infrastructures, which blurs the distinction between military and civilian targets.[87] [88]

Cyber warfare also produces problems for understanding the role of neutral states. If cyber attacks constitute a use of force, a belligerent is prohibited from issuing a cyber attack through the networks of a neutral state, and a neutral state's failure to resist the use of its networks by belligerents may make it a legitimate target for reprisals by the targeted country.[89] However, this conclusion assumes that a hostile cyber action is a violation of a state's neutrality.[90] A counterargument to this position asserts that, historically, violations of neutrality

[85] Ibid.
[86] Ibid.
[87] Heaton, J. Ricou. "Civilians at War: Reexamining the Status of Civilians Accompanying the Armed Forces." Air Force Law Review, 57 (2005).
[88] Ellis, Bryan W. "The International Legal Implications and Limitations of Information Warfare: What Are Our Options?" US Army War College Strategy Research Project, 10 April 2001.

[89] Ellis, Bryan W. "The International Legal Implications and Limitations of Information Warfare: What Are Our Options?" US Army War College Strategy Research Project, 10 April 2001.
[90] Ibid.

referred to physical violations of a nation's borders.[91] Because information attacks do not involve any physical intrusion, using or attacking a neutral nation's computer network might not violate its neutrality (thus, the neutral state is not required to resist belligerents' use of the state's computer networks).[92]

Domestic and International Policy

The current structure concerning cyber security within the United States government rests in the Department of Homeland Security (DHS). The DHS is home to the National Cyber Security Division (NCSD) which is responsible for the government's cyber security and critical infrastructure protection. This division of Homeland Security collaborates along with public, private, and international entities.[93] With concern to public policy, the United States is in the process of producing legislation which is outlined in National Security Presidential Directive (NSPD) 54, labeled the Cyber Initiative. As of May 2008, the initiative is before Congress.[94] Cyber security is also a high priority in the international community, as many nations are realizing the potentially dangerous effects of cyber attacks. On the international level, both the North Atlantic Treaty Organization (NATO) and the Council of Europe are taking steps to enhance policies on cyber security. The Council of Europe has developed the Convention on Cybercrime – an international treaty which seeks to unify standards concerning cybercrime

[91] Ibid.
[92] Ibid.
[93] Department of Homeland Security. 2008. Retrieved from the world wide web March 2008. <http://www.dhs.gov>
[94] United States. US House of Representatives. Committee on Homeland Security. Statement of Representative Bennie G. Thompson, Chairman: "The Cyber Initiative." Washington, D.C. 28 February 2008.

throughout the globe.[95] In addition, NATO has announced efforts in creating an official Policy on Cyber Defense.[96]

Domestic Framework

Historically speaking, western dependence on computer networks is a relatively new phenomenon that represents a foundational chunk of US government infrastructure. The nascent but colossal use of technology for communication and data transmission has caused a myriad security problems for policymakers. In 1998, RAND analyst Martin Libicki wrote: "Everywhere, computers and other digital devices have insinuated themselves into our lives. What was manual is now automated...what once stood alone is now connected to everything else...the potential consequences of deliberately induced system failure or corruption are vast."[97] Five years later, the US launched the 2003 *National Strategy to Secure Cyberspace,* but much debate continued.[98] Today, Libicki admits a lack of a national consensus on where to "draw the line" in distinguishing between different cyber activities.[99] National Defense University's Daniel Kuehl describes US cyber policy as trying to build a plane while simultaneously flying it.[100]

The cyber operations umbrella under which the United States currently operates might best be described as fragmented. The 2003 strategy document spoke to five "critical priorities," which included a national cyberspace security response system, a threat and vulnerability reduction program, security training, international cooperation and the securing of government cyberspace.[101] President George W. Bush wrote: "The cornerstone of America's cyberspace

---

[95] Council of Europe. Convention on Cyber Crime. Explanatory Report. 8 November 2001.
[96] North Atlantic Treaty Organization. Bucharest Summit Declaration. 3 April 2008.
[97] Libicki, Martin. "Ghosts in the Marchines?" US Foreign Policy Agenda, USIA Electronic Journal. 3:4 (1998).
[98] United States. The National Strategy to Secure Cyberspace. February 2003. http://www.whitehouse.gov/pcipb/
[99] Libicki, Martin. Personal interview. Washington, D.C.. 18 March 2008.
[100] Kuehl, Daniel. Personal interview. Washington, D.C.: 17 March 2008.
[101] United States. The National Strategy to Secure Cyberspace. February 2003. http://www.whitehouse.gov/pcipb/

security strategy is and will remain a public-private partnership. The federal government invites the creation of, and participation in, public-private partnerships to implement this strategy."[102] While laudable, the integration of many law enforcement institutions and policy bureaus with the private sector is challenging in the best of circumstances; the barriers are even greater when dealing with cyberspace, which can seem utterly intangible.

According to one expert, government actors are slowly warming toward opening communication channels, but serious challenges remain.[103] This tension may stem from the nature of the information technology industry, where "enormous resources" are available for government consumption, but there is little incentive to share information. When information is shared, the resulting dialogue is often unilateral: government entities have "tons of network data," but requests for information are often "relatively unsuccessful."[104] "Today, the attacker has all the advantages," the expert noted, and with some agencies rooted in traditional information practices, "how do you encourage that conversation?"

Public-Private Challenges

In the year 2006, the US Computer Emergency Readiness Team (US-CERT) received more than 23,000 reports of cyber incidents from a combination of public and private sources, a number that was surpassed in the first quarter of 2007 alone.[105] What percentage of attacks represented by those numbers is unclear; for example, Delaware state computer networks suffered over 3,000 attacks per day in 2005.[106] Assuming all fifty states suffered that volume, if

[102] Ibid.
[103] Personal interview: private industry cyber expert. Washington, D.C: 17 March 2008.
[104] Ibid.
[105] Garcia, Gregory. Prepared remarks by Department of Homeland Security Assistant Secretary for Cyber Security and Communications. 2007 RSA Conference in San Francisco, February 5-9, 2007.
[106] United States. Testimony of Delaware Senator Thomas Carper, Federal Financial Management, Government

not more, state government systems would face over 150,000 *per day.* This number would not include local, federal, or commercial networks, with the latter holding the bulk of critical national infrastructure.

Some private sector actors work with government agencies out of a self-described sense of "patriotism," but they also express the view that cyber defense is a national security issue, and therefore a federal government responsibility.[107] While the Federal Information Security Management Act (FISMA) of 2002 offered federal agencies an IT framework for assessing and reporting cyber events,[108] reporting requirements for the private sector are voluntary.

This may be shifting. In August 2006, new standards for cyber security across power networks, developed by the North American Electric Reliability Corporation, were submitted to the Federal Energy Regulation Commission (FERC), and published for public comment in the Federal Registry the following summer.[109] The eight specific Critical Infrastructure Protection (CIP) Reliability Standards span cyber asset identification, personnel training, physical security of cyber assets and incident reporting, among others.[110] Called a "milestone" by the FERC Chairman, the mandatory rules bind bulk power owners and operators to establish policies based on technical feasibility, replacing previous language requiring only "reasonable business judgment."[111] This was due in part to the Northeast Blackout of 2003, which drew attention to violations of the previous voluntary standards.[112]

Information and International Security Subcommittee before the United States Senate Committee on Homeland Security and Government Affairs, 109th Congress. 19 July 2005.

[107] Personal interview: private industry cyber expert. Washington, D.C. 17 March 2008.

[108] United States. Executive Office of the President. "Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting." OMB Memorandum for Heads of Executive Departments and Agencies from Director Joshua Bolton. August 6, 2003.

[109] "FERC approves new reliability standards for cyber security." News Release, FERC.gov, 17 January 2008.

[110] Ibid.

[111] Ibid.

[112] Stanton, James R. "Cyber Security under the NERC Reliability Standards." IT Compliance Magazine, Spring 2007.

> While the causes of the 2003 blackout were not the result of a cyber attack, similar damages and cascading events could result from coordinated intrusions of the infrastructure that monitors and controls the interconnected electric transmission grids. Obviously, these types of events not only result in high costs and endangerment to the public, but also represent significant breaches in national security.[113]

Effective April 7, 2008, bulk power operators finding themselves under new federal regulations for cyber security may signal a harbinger of future regulations across other industries.[114] Unlike pollution credits, where certain industries can purchase the "right" to pollute above allowable thresholds, cyber actions create negative externalities that are not easily mitigated, and can be both immediate and tangible.

Existing Structures

Issued by President George W. Bush, Homeland Security Presidential Directive 23, and NSPDs 16 and 54, concern cyber security and operations.[115] These mandates are outside of the scope of this research.

The DHS's National Protection and Programs Directorate is the home of US-CERT (United States Computer Emergency Readiness Team),[116] a public-private partnership located in Washington, D.C. which represents the cyber "operational" arm of DHS.[117] Responsible for implementing the 2003 *National Strategy to Secure Cyberspace*, both private and public entities can report cyber incidents to US-CERT via the Internet, secure email, telephone or postal

[113] Ibid.
[114] Hershfield, Mark. 2008. "Mandatory Reliability Standards for Critical Infrastructure Protection." E-mail to Stephanie Silva, May 5, 2008.
[115] Federation of American Scientists. "National Security Presidential Directives, George W. Bush Administation." May 5, 2008.
[116] Department of Homeland Security. "Leadership." Retrieved from the world wide web March 2008. <http://www.dhs.gov/xabout/structure/gc_1157655281546.shtm?>
[117] US-CERT. (n.d.). Retrieved from the world wide web in February 2008. < http://www.us-cert.gov/aboutus.html>

mail.[118] Established in 2003, US-CERT is a separate entity from Carnegie Mellon University's CERT® Coordination Center, which was established in 1998 through a Defense Advanced Research Projects Agency (DARPA) initiative.[119] Carnegie Mellon's CERT®[120] is "an organization devoted to ensuring that appropriate technology and systems management practices are used to resist attacks on networked systems and to limiting damage and ensure continuity of critical services in spite of successful attacks."[121]

Despite their status as separate organizations, US-CERT and Carnegie Mellon's CERT® coordinate both with each other and over 250 individual cyber security centers worldwide who use the term "CERT," or variations thereof, in their name.[122] Added to the conglomeration of US-CERT partners are also various Information Sharing and Analysis Centers (ISACs), some of which are private entities that operate on a contractual basis with their members,[123] [124]and others who partner with the federal government.[125]

Inside the federal government itself is the Critical infrastructure Warning Information Network, or CWIN. The voice and data network exists to support secure communication among government actors, private entities and trusted foreign sources in the event of significant network disruption. For combined fiscal years 2005 and 2006, CWIN represented a total cost of over $24

[118] US-CERT. (n.d.). Retrieved from the world wide web in March 2008. <http://www.us-cert.gov/contact.html>
[119] Software Engineering Institute, Carnegie Mellon. 2008. "The CERT FAQ." <http://www.cert.org/faq/cert_faq.html>
[120] Carnegie Mellon University's CERT is a trademarked name, and is not an acronym.
[121] Software Engineering Institute, Carnegie Mellon. 2008. "The CERT FAQ." <http://www.cert.org/faq/cert_faq.html>
[122] US-CERT. (n.d.). Retrieved from the world wide web in February 2008. <http://www.us-cert.gov/aboutus.html>
[123] IT-ISAC. 2006. <https://www.it-isac.org/aboutitisac.php>.
[124] IT-ISAC interview, Washington, D.C. 17 March 2008.
[125] US-CERT. (n.d.). "Related Resources: Information Sharing and Analysis Centers." <http://www.us-cert.gov/resources.html.>

billion, with some cyber security professionals questioning its return on investment. According to one expert, the extent to which CWIN is efficacious, or holds any value at all, is unclear.[126]

Legislation, Jurisdiction, Management

Depending on the nature of a cyber incident, multiple agencies might be called to respond, from the Department of Homeland Security and the Department of Energy, to Coast Guard Intelligence and the National Reconnaissance Office.[127] Cyber event jurisdiction is not always immediately clear: According to FBI Supervisory Special Agent Matt Fine, the rush to categorize incidents is purposely avoided.[128] Cases may develop over several days, with their evolution dependent on the cyber actor; incident complexity sometimes demands a more amalgamated lens than traditional law enforcement methods.[129]

One issue plaguing federal law enforcement is the current set of statutes under which operational authority is granted. Titles 10, 18 and 50 of the United States Code (USC) address criminal matters facilitated via electronic means, but their scope can be limiting.[130] [131] For example, the FBI's prosecution of everything from Internet financial fraud to child exploitation falls under Title 18, Chapter 47, subsections §1028, §1029, §1030, and §1037.[132] The wide operating scope of the statutes may serve as a hindrance in some cases, as the growing complexity of cyber incidents calls for greater legislative diversity when addressing cyber

[126] Personal interview: private industry cyber expert. Washington, D.C: 17 March 2008.
[127] "The Computer Intrusion Section: FBI Cyber Division." Federal Bureau of Investigation booklet. Obtained March 17, 2008., J. Edgar Hoover Building, 935 Pennsylvania Avenue, NW, Washington, DC 20535-0001
[128] Fine, Matt. Personal interview. Washington, D.C.: 17 March 2008.
[129] Ibid.
[130] Ibid.
[131] Cornell University Law School, US Code Collection, Title 18.
[132] Fine, Matt. Personal interview. Washington, D.C.: 17 March 2008.

needs.[133] Adaptation to the cyber actor, a key to fighting cyber crime, [134] may require greater malleability among jurisdictional assignments as well.

A second challenge lies within cyber infrastructure security management. One expert spoke of the Central Intelligence Agency (CIA) and the National Security Agency (NSA) as holding "too many cooks in the kitchen," while DHS has been openly criticized on Capitol Hill and by the press for management problems.[135] When the position of "Assistant Secretary for Cybersecurity" was created to replace the former "National Cyber Security Division Director," one official was quoted as noting that a mere title elevation would not solve agency challenges.[136] In light of supervisory issues, internal management promotions at DHS have also been openly questioned by members of Congress.[137]

A third concern relates to the armed forces. The 2003 DOD "Information Operations Roadmap" detailed institutional concerns about cyber vulnerabilities, stating: "Networks are growing faster than we can defend them….The sophistication and capability of both hackers and nation-states to degrade system and network operations are rapidly increasing."[138] The report recommended a strategy based on the premise that the Department of Defense will "'fight the net' as it would a weapons system" and included "well-integrated Computer Network Attack/Computer Network Defense [CNA/CND] efforts that permit us to maximize opportunities for CNA and minimize vulnerabilities in our CND efforts."[139] The 2006 establishment of the US Air Force's Cyber Command by the Air Force was followed by official comments delineating

[133] Fine, Matt. Personal interview. Washington, D.C.: 17 March 2008.
[134] Ibid.
[135] Ibid.
[136] Lemos, Robert. 2005. "Cybersecurity Czar will have hard road ahead." Security Focus, June 2, 2005.
[137] Thompson, Bennie G. Letter to Secretary Michael Chertoff. 01 February 2008. One Hundred Tenth Congress, US House of Representatives, Committee on Homeland Security, Washington, D.C. 20515.
[138] United States. Department of Defense. "Information Operations Roadmap," October 30, 2003, p. 44.
[139] Ibid, pps. 45-46.

the cyber realm as both defensive and offensive in nature.[140] According to officials at the Pentagon, the United States military is in need of standardized "cyber" rules of engagement to fulfill these growing operational responsibilities.[141] The streamlining and defining of cyber standards across the armed forces would, by logic, promote efficiency across logistics and operations. However, unless all government agencies agree to use the same, or complimentary, cyber Rules of Engagement (ROE), an abundance of problems will remain.

International Framework

In late April of 2007, the small and technologically savvy country of Estonia fell victim to a series of cyber attacks which nearly shut down their network infrastructure and financial institutions. The majority of the cyber attacks were of a DDOS variety and were successful in disrupting Estonia's economic and social structures, caused damages estimated in the millions. These cyber attacks brought the issue of cyber security and protection of national infrastructure to the forefront of international news, and was referred to as the "watershed of awareness of the vulnerability of modern society"[142] by the principal deputy assistant Secretary of Defense for Networks and Information Integration at the Pentagon. Since Estonia is a member country of the North Atlantic Treaty Organization (NATO), the attacks also caused a new wave of attention from NATO and compelled the organization to increase its focus on the issue of cyber security.[143]

---

[140] Lopez, C. Todd. "Fighting in cyberspace means cyber domain dominance." Air Force Print News, 28 February 2007.
[141] Hare, Forrest. Personal interview: Washington, D.C. 17 March 2008.
[142] Landler, Mark, and John Markoff. "Digital Fears Emerge After Data Siege in Estonia." New York Times, 29 May 2007.
[143] Ibid.

Since the attacks, NATO has sharpened its efforts on cyber security and is currently in the process of creating a framework for cyber defense. In the Bucharest Summit Declaration, released on April 3, 2008, NATO announced their efforts to adopt a Policy on Cyber Defense. NATO is focused on developing the structures and authorities to carry out the policy.[144] The Policy on Cyber Defense will underline the need for the protection of critical information and infrastructure, as well as developing and using shared best practices. The policy will also accentuate the need for the assistance of Allied members in the occasion of a cyber incident, and increase cooperation between NATO and national authorities. This is yet another step in the international effort to help deter cyber crime.[145]

Another international body, The Council of Europe, has also initiated efforts to help thwart cyber crime. The Council of Europe was founded in 1949 and seeks to develop common and democratic principles throughout Europe, based on the European Convention and human rights issues. Currently, the Council of Europe has 47 member countries and five observing countries, including the United States.[146]

In November of 1996 the Council's European Committee on Crime Problems began its agenda to address the issue of cyber crimes, and established a committee of experts to study the issue. One of the primary reasons for the establishment of this committee was the realization that criminal law needed to keep pace with the vast technological advancements and their potential misuse that could cause harm and damage. Continuing their quest at examining this issue, a new committee was developed in February 1997 called the *Committee of Experts on Crime in Cyberspace*. After numerous meetings, the final draft was adopted, and the Convention on

[144] North Atlantic Treaty Organization. Bucharest Summit Declaration. 3 April 2008.
[145] "NATO Agrees Common Approach to Cyber Defense." EurActiv.com. 4 April 2008. April 2008 <http://www.euractiv.com/en/infosociety/nato-agrees-common-approach-cyber-defence/article-17137 >
[146] Council of Europe. "About the Council of Europe." Retrieved from the world wide web March 2008. <http://www.coe.int>

Cybercrime was brought into force on July 1, 2004. The Convention's principal concern is to address the continuing problems of cyber crime and establish a unified policy intended to protect society against illegal cyber activity. The Convention is designed to aid legislation and encourage international cooperation concerning cyber crime.[147]

Past and present US administrations worked alongside the Council of Europe to draft the Convention on Cyber Crime; the Convention was introduced into the United State's Senate in November of 2003, and was issued a hearing by the Senate's Foreign Relations Committee.[148] In August of 2006, the Convention on Cyber Crime was ratified by the United States Senate. US Attorney General Alberto Gonzales stated, "the Cyber Crime convention – the first of its kind – will be a key tool for the United States in fighting global, information-age crime."[149]

The Council of Europe Convention on Cybercrime is the only legally binding international treaty which addresses cyber related crime. NATO has expressed interest in developing a framework concerning cyber security, and is currently in the process of creating an official agreement.

Foreign Policy Considerations

Even with a treaty of mutual legal assistance, parties generally retain exceptions that permit the nation to refuse cooperation under certain circumstances.[150] Moreover, when nations cooperate, those nations must share an understanding of the standards of proof needed before an

[147] Council of Europe. Convention on Cyber Crime. Explanatory Report. 8 November 2001. <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>
[148] Archick, Kristin. "Cybercrime: The Council of Europe Convention." Congressional Research Service Report for Congress. 28 September 2006.
[149] Walker, Carolee. "US Senate Votes to Ratify Cybercrime Convention." America.gov. 7 August. 2006. March 2008 <http://www.america.gov>
[150] Ellis, Bryan W. "The International Legal Implications and Limitations of Information Warfare: What Are Our Options?" US Army War College Strategy Research Project, 10 April 2001.

act can be taken or an illegitimate actor apprehended. To access information regarding the nature of cyber attack, authorities must be able to reverse-trace back through the computers and networks from which the attack came. In order to have an effective reverse-trace, the United States must obtain assistance from government and civilian entities in the countries in which the computers were used. Obtaining this assistance may be difficult and time-consuming. As time passes, the fragile digital evidence can disappear before investigators obtain the requested assistance. Additionally, if the other implicated countries have not criminalized computer malfeasance, obtaining assistance from the native authorities may be impossible.[151]

US criminal statutes and foreign criminal statutes apply to information operations activities. A state's domestic criminal law directly affects the assistance that the nation can provide in suppressing hostile cyber acts committed by persons operating in the state or country's territory, and can also limit information operations conducted in that state's territory or routed through the states's networks.[152] In one example, some nations have enacted data protection codes that forbid the transmission of certain personal data to countries that do not provide sufficient protection for the data. [153]

One option lies in the support and development of an extradition regime for information attacks.[154] Extradition can be accomplished by international treaties, though generally individuals will be exempted from extradition if they are nationals of the country in which they are found. Also, many extradition treaties contain double-criminality clauses, which state that persons will only be extradited if the act was considered a crime in both states.

---

[151] Brenner, Susan W. "At Light Speed: Attribution and Response to Cyber Crime/Terrorism/Warfare." The Journal of Criminal Law and Criminology , 97:2 (2007).
[152] Ellis, Bryan W. "The International Legal Implications and Limitations of Information Warfare: What Are Our Options?" US Army War College Strategy Research Project, April 10, 2001.
[153] Ibid.
[154] Ibid.

NATO is a classic example of international cooperation regarding the use of force. One of NATO's core principles (codified in Article 5 of the NATO agreement) is that an attack on one NATO member-state is an attack on all NATO members. However, the case of Estonia provides a precedent that in regard to cyber warfare, that principle does not apply. A cyber attack on one NATO-member is not an attack on all. The law of war, however, could be modified to clarify which cyber activities constitute "aggression," "intervention," "use of force," "direct participation in hostilities," "armed attack," and "act of war."

Major military states could jointly issue a non-binding statement of principles that define which specific cyber activities constitute which legal categories.[155] The concept of what constitutes damage to enemy personnel and equipment needs to be broadened to explicitly cover damage to information residing within computer networks. Attacks on information processing computer systems that destroy, damage, or alter information can result in significant damage to an economy or military. The international community should publicly acknowledge that attacks on information systems do cause damage and ensure that attacks on computer networks during the course of an international armed conflict are restricted to legal combatants and regulated by the law of war.[156] Additionally, by coordinating their understandings and practices regarding cyber activities, states can establish a pattern of state practice that could ripen into customary international law over time.[157]

Computer Network Attack Exploitation (CNAE) may implicate the International Telecommunications Union (ITU), which is founded on the International Telecommunications Convention (ITC). The ITU (and ITC) govern international wire and radio frequency

[155] Heaton, J. Ricou. "Civilians at War: Reexamining the Status of Civilians Accompanying the Armed Forces." Air Force Law Review, 57 (2005).
[156] Ibid.
[157] Ibid.

communications. Because they are primarily concerned with promoting interoperability and reducing interference the ITU and ITC may not substantially limit CNAE.[158] However, ITU regulations are applicable to CNAE that use the electromagnetic spectrum or international telecommunications networks.

Under the ITU, the broadcasting stations in one nation are prohibited from interfering with the broadcasts in another state (on the second state's authorized frequencies). Governments are also obliged to protect the secrecy of international correspondence, though they retain the right to stop radio or wire transmissions for national or domestic security purposes.[159] Wartime communications are not protected because the rules against interference do not apply to belligerents.[160] In peacetime, violations of the ITU regulations only have limited repercussions. If CNAE violate ITU regulations, such activities may be considered merely a breach of contractual obligation under the treaty, which would not justify a self-defense or use of force response.[161]

Characterizing Cyber Acts

It is the purpose of this paper to produce a universal framework for understanding the issues inherent across cyber actions. A few scholars have begun to offer such frameworks for understanding cyber warfare, and this paper will aim to incorporate and expand upon the notions which they have put forth. Most notable among these attempts to provide a multi-factor approach is the work of Michael Schmitt, a noted Professor of International Law who enumerated a number of criteria toward cyber action analysis, such as presumed Legitimacy:

[158] Ellis, Bryan W. "The International Legal Implications and Limitations of Information Warfare: What Are Our Options?" US Army War College Strategy Research Project, 10 April 2001.
[159] Ibid.
[160] Ibid.
[161] Ibid.

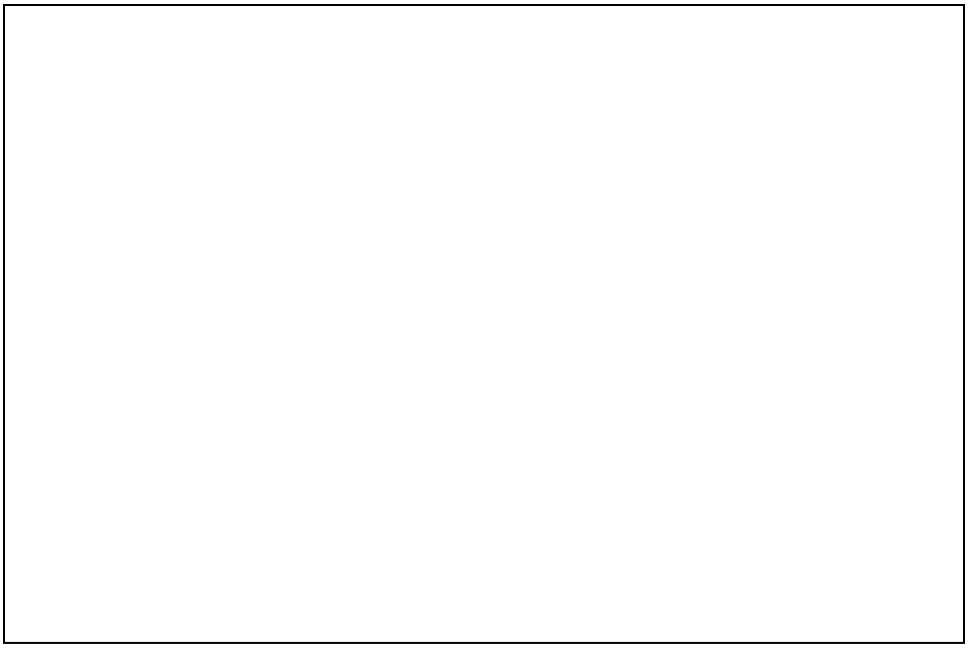


Figure 1: Schmitt's Presumptive Legitimacy Measurement

> State actors have a monopoly on the legitimate use of kinetic force, while other non-kinetic actions—attacks through or in cyberspace— often are permissible in a wider set of circumstances; actions that have not been the sole province of nation-states are less likely to be viewed as military.[162]

Writing in 1999, Schmitt argued "Computer network attack represents a new tool of coercion in the international arena, one that is fundamentally different from those previously available."[163] According to Schmitt, there was no question that the field of Information Operations would require a new framework, however, he also acknowledged that such universal agreement was not likely in the immediate future, but through gradual policy change.[164] Schmitt's work is widely referenced in the peer-reviewed journals of Computer Science and Engineering, most notably by scholars Thomas Wingfield and James B. Michael.

[162] Schmitt, Michael. "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework." Institute for Information Technology Applications, Research Publication 1, June 1999.
[163] Ibid.
[164] Ibid.

For purposes of this project, it is not recommended that the Schmitt analysis be adopted wholesale, but rather that it ought to provide the foundation for a framework which also includes some prominent alterations. For example, the framework presented in this paper includes a motivation-factor, which is absent from the Schmitt analysis. It also excludes the Schmitt factors concerning directness and immediacy, as those factors seem to be best understood as sub-characteristics of a broader category which this research team terms “Effects.” A number of other factors articulated in the Schmitt analysis have been renamed in an attempt to enhance the breadth and comprehensibility of those factors.

Similar to the analytic frameworks which have preceded this writing, the framework presented in this paper is intended to provide military personnel and foreign relations personnel with a common, uniform understanding which will enable them to focus on particular aspects of hostile cyber acts while maintaining awareness of how those aspects relate to other critical factors. Additionally, the individual factors which comprise this framework should further illuminate specific aspects of hostile cyber acts, such as the effects of hostile cyber acts on national interests, the nature of the actors whom states wish to deter, the nature of the acts which states wish to deter, as well as several additional aspects.

Critical Factors

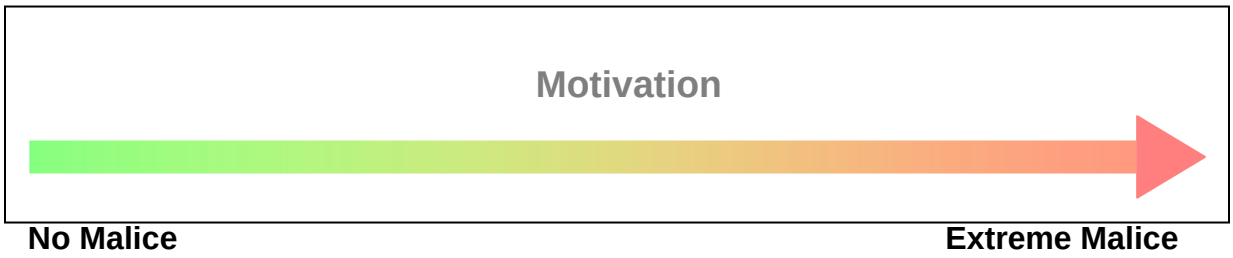


Figure 2: Motivation Continuum

Motivation is a complex concept which occurs in a dynamic and evolving context. Some social psychology literature surrounding weapons of mass destruction indicates that an actor's decision to use such revolves around whether or not their actions will involve killing "innocent" noncombatants.[165] After an actor makes this decision, choosing to employ one technology instead of another is a much less significant decision, and one often driven by opportunity and expertise rather than by social or behavioral considerations.[166]

Although studied in several disciplines, there is no universally-accepted definition of motivation.[167] A 2007 Defense Threat Reduction Agency report adopted the following points, which was said to encompass the consistent concepts across various fields: "the forces, either within or external to a person or group, that arouse enthusiasm and persistence to pursue a certain course of action."[168] The benefits of this definition, as asserted by the authors, are that the definition (1) recognizes that motivation can be influenced by either internal or external forces, (2) remains neutral in regard to the nature and origin of those forces, (3) highlights the critical

[165] United States. Defense Threat Reduction Agency. Terrifying Landscapes: A Study of Scientific Research Into Understanding Motivations of Non-State Actors to Acquire and/or Use Weapons of Mass Destruction by Kay Hayden, 2007.
[166] Ibid.
[167] Ibid.
[168] Ibid.

role of persistence, and (4) suggests both goal-orientation and directed-action without limiting applicability to rational actor approaches.[169]

The motivational factors of cyber actors – political, social, cultural, economic, psychological, and so forth – are important to developing a behavior-characterization model.[170] Motivations are core components of the initial decisions about technology acquisition, choice of technologies, and delivery mechanisms.[171] As these motivations strongly influence the degree of effort that an actor may be willing to expend in overcoming obstacles, they must be considered in developing effective dissuasion and deterrence strategies.[172] To understand the dynamic nature of cyber actors' motivations, analysts must understand that behavior is the result of a broad combination of factors.[173]

Cyber actors might be motivated to act out of personal interest, ideological interest, political interest, national interest, or no particular interest at all. Moreover, the motivations of cyber actors differ from one another on a critical component: the degree of malice. Cyber activity conducted with no underlying motivation, or simply out of personal interest, may be less malicious than cyber activity conducted in pursuit of political or national interests. However, associations between types of acts and degree of maliciousness are only generalities. When the two factors diverge, the critical component for understanding the nature of the cyber act is not the specific interest of the cyber actor, but rather the degree to which the cyber act is malicious.

Some cyber acts may be without motivation, for example, a person randomly clicking hyperlinks absent a specific goal. One step up from such an example would be a cyber actor with

---

[169] Ibid.
[170] Ibid.
[171] Ibid.
[172] United States. Defense Threat Reduction Agency. Terrifying Landscapes: A Study of Scientific Research Into Understanding Motivations of Non-State Actors to Acquire and/or Use Weapons of Mass Destruction by Kay Hayden, 2007.
[173] Ibid.

an identifiable motivation, but one without practical significance; for example, a person reading online celebrity news is not noteworthy for issues of national security. In other instances, cyber actors may be motivated by personal interests, which themselves may be legitimate or illegitimate. A cyber actor paying bills online is clearly pursuing a personal interest, while a person siphoning money from another person's bank account is pursuing a private interest. Ideological interests, political interests, and national interests are also potential motivations driving cyber actors; for example, the desire to see more members of one political party seated in Congress or the desire to inhibit judicial appointments made by a particular executive.

Beyond personal interests, motivations of cyber actors become increasingly relevant to determinations as to how the cyber act ought to be construed. Even though illegitimate cyber acts motivated by personal interests are likely to constitute criminal activity, it is unlikely that illegitimate cyber acts motivated by personal interests will ever amount to a cause for concern of a country's military. Conversely, cyber acts motivated by political, ideological, or national interests will likely have greater potential for the type of actions with which defense agencies would be concerned.

Admittedly, the degree of malice can vary across motivations, and defining exact thresholds would quite likely result in blurred lines between supposedly different motivations. Though judging malice will require some subjectivity, the degree of malice behind *Motivation* is the decisive issue for this critical factor, as it relates to violent behavior. By focusing on motivation, this framework attempts to incorporate a causal antecedent to violent cyber behavior.[174] As a psychological variable, a cyber actor's motivation may not be apparent from

[174] Abbot, Marrianne & Jill Egeth. "Intentions, Motivations, and Violent Non-State Actors." Powerpoint presentation, Military Operations and Research Society, MITRE Corporation. 5 February 2008.

the forensic evidence alone. However, through a conjunction of intelligence sources and techniques, it may be feasible to reasonably estimate a cyber actor's motivation.

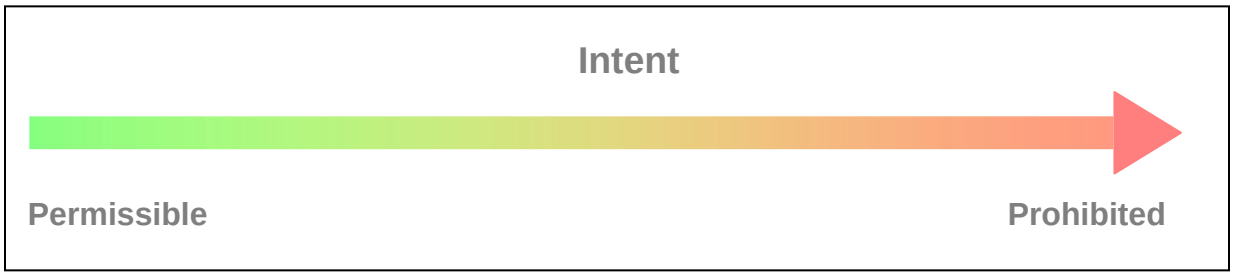


Figure 3: Intent Continuum

Intent refers to the tactical objective of a cyber actor and describes the objective of an act, regardless of what the act does or does not result in. Should an act fail or produce negligible results, the difference between Intent and actual *effect* is clarified. This does not mean, however, that an unsuccessful cyber action is automatically less serious than a *completed* one; if a hostile state attempted to cause major damage or death via a cyber act but was ultimately foiled, the seriousness of the intent would not necessarily be nullified.

As with the other factors in this proposed framework, intentions of cyber actors fall along a continuum. The continuum is characterized by the presumptive legitimacy an act would carry in the international and domestic communities, ranging from permissible to prohibited.[175] For example, acts in self-defense might be considered permissible, while an actor intending to produce property damage might be portrayed as prohibited.

According to the field of Information Assurance, a cyber actor's intent carries the potential to be analyzed via technical means. Under this understanding, an attack may do any of four things: breach confidentiality, assail availability, compromise integrity or subvert control.

[175] Schmitt, Michael. "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework." Institute for Information Technology Applications, Research Publication 1, June 1999.

Breaching confidentiality would involve the unauthorized access to secured information. From an historical perspective this could be likened to espionage in an international context. Acts of espionage are significant threats to a country's secure information, but in the international community are not strongly prohibited against and have largely been characterized by a "let the best competitor" win attitude. Thus breaching confidentiality is not an extremely prohibited act. Assailing availability is the disabling of network resources, and is frequently accomplished through the utilization of DOS attacks. Such tactics have caused much political outrage as the attacks on Estonia exemplify. This indicates that these types of attacks are much more prohibited and restrictive than broaching confidentiality.

Compromising integrity is the altering of secure data, thus reducing the integrity or trustworthiness of the data. This type of attack is much less permissible than simple espionage as it involves the defrauding of whatever next utilizes the data. This also contains a significantly higher level of danger as the actor would not be completely knowledgeable of how the data will be used in the future. Finally, subverting control of cyber entities takes one of two forms. The first is the utilization of an unauthorized service, and the second is seizing complete control of a system or server. Utilizing an unauthorized service may be as simple as hijacking a network router to only handle the actor's traffic, or placing a virus in a computer which then spreads it to others. In these circumstances the system's resources are being subverted by the actor but the system still retains a certain level of autonomy. Seizing complete control of a system in many cases would be attaining root access, allowing the actor near ultimate control of the system's utilization. This would be a much less permissible act because instead of just hijacking excess resources the entire system is compromised.

Also carried by the Intent factor is the tactical importance of determining a relevant defense. According to Lowry, "An understanding of the cyber-adversary's goals and objectives for targeting a particular system constrains the space of attack vectors and identifies opportunities for effective defense."[176] According to experts, the importance of assessing intent via "zero day" analysis – recognizing and charting an attack during the first twenty-four hours – cannot be overstated, though its execution is admittedly challenging.[177]

While Intent can be difficult to divorce from effects forensically, often an actor's intent will become obvious as the cyber attack matures, though such growth is usually undesirable. Naturally, the attack target is also a significant area, as it provides a vehicle to shape underlying goals. Finally, the intent may need to be further molded by intelligence sources outside of the forensic evidence pattern. In summary, this research has indicated Intent as the defining characteristic of action legitimacy, which itself determines what response, if any, may be necessary or appropriate.

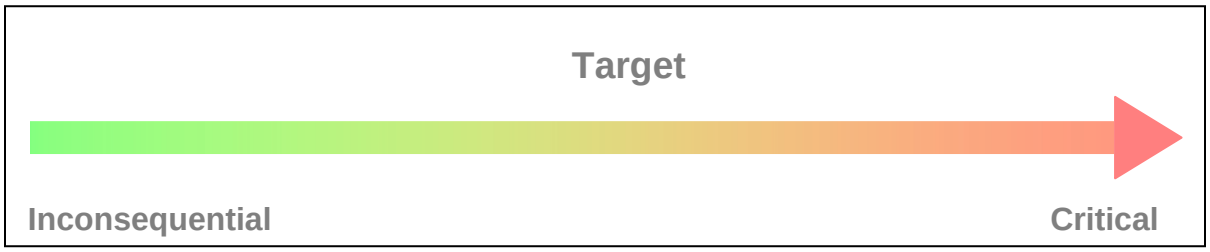


Figure 4: Target Continuum

Another notable factor necessary for characterizing hostile cyber acts is the target of the act. Target refers to the cyber network, system, infrastructure, or information nexus which is

[176] Lowry, John. "Technical Considerations in Cyber Conflict," Journal of Cyber Conflict Studies, Vol. 1, No. 1, Arlington, VA. Cyber Conflict Studies Association, November 2005.
[177] Personal interview with software experts. Washington, D.C. 18 March 2007.

subjected to the cyber act. Types of targets in cyberspace range from personal websites to secure government information. There is no exhaustive list of cyber targets, due to the evolving nature of technology and corresponding technological dependence.

Historically, geographical considerations played a prominent role in the characterization of a hostile act, such as when an attacker violated the physical territory of a state (i.e., crossing a state's border without that state's consent). Unlike the physical realm where an actor's affiliation may be the most significant factor in characterizing a hostile act, according to Jensen, "In the case of critical national infrastructure, it is the target of the attack that should define the threat and appropriate response, not the attacker."[178]

Some international legal scholars have begun to examine the role of the target of an attack in regard to hostile cyber acts. Schmitt described an act's degree of "invasiveness" as a notable factor relevant to characterizing a hostile act.[179] Although Schmitt's description of "invasiveness" emphasized geographic borders, the description also identified the significant notion of intrusion onto a state's rights.[180]

Numerous complications arise from relying on physical boundaries to distinguish various cyber acts. Servers and communication networks are often completely anonymous to the individual utilizing them. According to Litman:

> The Internet is quickly making geographic borders metaphorical. Where actions with legal significance consist of streams of electrons taking varying paths among computers all over the world, we need to adjust our laws' conception of "place." There are a variety of rules we could adopt to fit events occurring over the Internet into pre-existing categories; there are a variety of alternative models we could adopt instead. Some of the conventional models, though, are clearly

[178] Jensen, Eric. "Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense." Stanford Journal of International Law, Vol 38, pp 207-240.
[179] Schmitt, Michael. "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework." Institute for Information Technology Applications, Research Publication 1, June 1999.
[180] Ibid.

> unworkable: We don't now have, and seem unlikely to develop, any way to put border guards between computers located in different jurisdictions to examine all of the electrons streaming through. Governments, lawyers, and legal scholars are just beginning to think about these questions in a systematic way.[181]

Because of the concerns regarding reliance of physical boundaries to define cyber acts, the notion of intrusion onto a state's rights may be a more adaptable metric for distinguishing between the targets of cyber attacks. After all, the reason why physical intrusions have historically been regarded as significant determinants for characterizing hostile acts lies not in the mere fact that a border was crossed, but rather in the fact that a border was crossed *without the consent* of the target state. Thus, to characterize hostile cyber acts, targets which represent higher levels of security for a nation should be understood to also represent greater "invasiveness" or intrusion against the rights of that state. For example, two separate attacks, each targeting a different communication network, might be characterized differently in regard to degree of intrusiveness if one attack targeted the network of a local Internet Service Provider (ISP) and the other attack targeted a federal emergency response network.

There are three standards by which the degree of intrusiveness can be measured. First, a technical standard would consider the nature and extent of protections and precautions guarding a system. While this standard may not always provide a perfect correlation for the degree of intrusiveness, it will generally identify highly critical systems as well protected and less critical systems, which lack protection.Under this standard, the nature and extent of defenses guarding a system (and correspondingly, the nature and extent of defenses successfully circumvented) would indicate the level of intrusion that a cyber act represents.

[181] Litman, Jessica. "Symposium: The Internet: Law without borders in the information age." The Wayne Law Review, 43 (1996), pp 95-98.

The second standard for measuring degree of intrusiveness is the danger that disruption of a system would produce. If the physical safety of human beings relies on a particular system, degree of intrusiveness would be exceedingly high. Even a minor disruption of such systems could produce significant negative consequences. Lastly, the standard for measuring degree of intrusiveness is the relationship of a system to the overall security of a nation. In the domain of domestic security, numerous conversations exist concerning this notion of critical security infrastructure and which targets constitute critical infrastructure.

Among these measurement options, technical tools to capture the level of intrusion provides the most objective standard for discerning hostile cyber actions. The United States government already maintains a system of security clearances, and that clearance system is one form of metric which can apply whether the system be public, Sensitive, For Official Use Only, Classified, or Top Secret. These classifications naturally transfer to the networks created for such classifications (NIPRNET, SIPRNET and JWICS networks). Other technical considerations could include encryption schemas or the use of firewalls.

Measuring intrusiveness can also be judged by the amount of damage a disruption causes. One significant feature of cyber actions not generally shared with kinetic weapons is the large amount of non-specificity an attack contains.

> Computing and networking systems can have a large amount of homogeneity. This is apparent in many Internetworking environments where a near monoculture of Microsoft Windows, Intel processors, and CISCO networking equipment is in use. No matter where it is encountered, homogeneity can make CNA fine-grained targeting extremely difficult. Furthermore, there can be intimate and difficult to discover dependencies between systems such that even the most specific targeting may 'bleed over' on to unrelated systems.[182]

[182] Lowry, John. "Technical Considerations in Cyber Conflict," Journal of Cyber Conflict Studies, Vol. 1, No. 1, Arlington, VA. Cyber Conflict Studies Association, November 2005.

Cyber tools such as worms and viruses are self-replicating and directing pieces of software. Thus, they often produce uncontrolled and unexpected consequences. While an attack may target a single machine in a critical system, there exists the danger that the means of the cyber attack will similarly infect other vulnerable machines in that system. As a result of this potentiality, the intrusiveness of a target is highly dependent upon the particular dangers that exist from any, especially undirected disruptions of the system.

In the 1997 *Report to the President's Commission on Critical Infrastructure Protection*, seven specific industries were identified as critical infrastructure areas: Information and Telecommunications, Electric, Oil and Natural Gas, Banking and Financial Services, Transportation, Drinking Water, and Emergency Services.[183] For example, even a minor attack on the Emergency Services sector may endanger lives, thus containing a high level of immediacy.

Bearing in mind the above discussion, analyzing the nature of the target can assist decision in partially discerning some characteristics of the action, including the level of sophistication as well as the amount of forethought and preparation. If a target is highly defended, classified and critical to national infrastructure, an attack would seem to suggest that the actor is well informed and highly strategic. Such information might improve the possibility of attribution to a cyber actor and might additionally help identify some aspects of the actor's intent. If a target is a well known control structure for critical communications or power management, disruption of that target might suggest an intent to produce physical or financial damage. Alternatively, if a target is a significant information cache, such as a national research lab, an attack on such a system might suggest some level of espionage. Thus, consideration of

[183] Alexander, Yonah, and Michael Swetnam. Report to the President's Commission on Critical Infrastructure Protection: Cyber Terrorism and Information Warfare. Vol. 3. Dobbs Ferry, New York: Oceana Publications, 1999.

the target of a cyber attack not only contributes to characterizing the nature of a hostile act but also helps illuminate other factors which contribute to the characterization.

Ultimately, the degree to which the target of a cyber action compromises the sovereign rights of a state is essential to determining the nature of the attack. The degree to which an attack intrudes upon the rights of a state can best be calculated by considering the amount of protection surrounding the target, the relationship of the target to the overall security of the United States, and the amount of damage that disruption of the target could produce. The level of potential harm to the security of the nation is paramount.

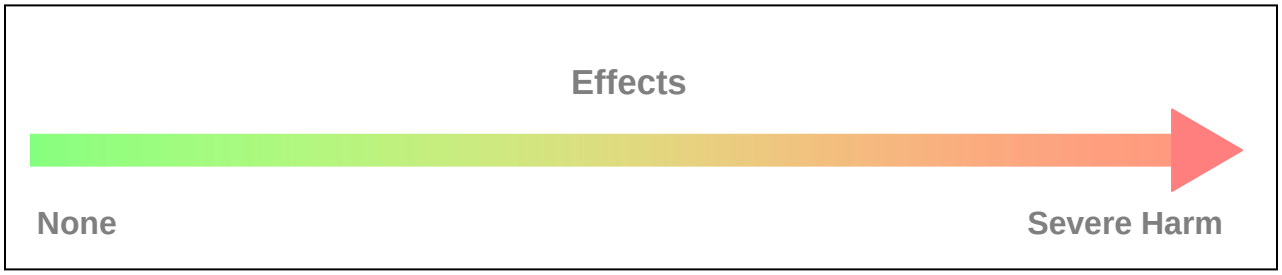


Figure 5: Effects Continuum

Effects are the final results of a cyber act. Effects are judged upon a permissibility spectrum that places emphasis on the magnitude of the action. The effect spectrum is closely related to the intent spectrum; where the intent is the goal that the actor wished to accomplish, the effects include said accomplishment or failure, and any other consequences of the act. Some effects of hostile acts in cyberspace include information manipulation, system disruption, property damage, financial loss, and human harm.

Generally, the effects of an act may be more readily measurable than the other factors as they can directly impact objects or resources which a known, tangible value. However, there also exist many effects that are not as readily quantifiable and deal with intangible characteristics,

such as psychological and social considerations. For instance, if an act causes a financial institution's website to be inoperable, a number of effects might be considered when quantifying the total effect. One effect would be financial loss as a result of transactions that were not completed during the downtime. This effect can be readily estimated and is therefore a primary effect of the act. The act may also damage the reputation of the financial website causing clients to do business with other financial institutions that are viewed as more reliable. This effect is more difficult to quantify and may take an extended amount of time to be realized, but does not necessarily lessen the importance of the effect.

The world’s economic powers are heavily dependent not only on technology, but on the interdependency of each other, which may also act as a deterrent to hostile acts inside and outside the cyber realm. A severely hostile cyber act, or the imminent threat thereof, may raise awareness worldwide and consequently act as a catalyst for international cooperation. This will foster development of international agreements concerning cyber policy. In order to foster such policy initiatives, the need for universal – or complimentary – cyber event measurement systems are necessary.

Methodology

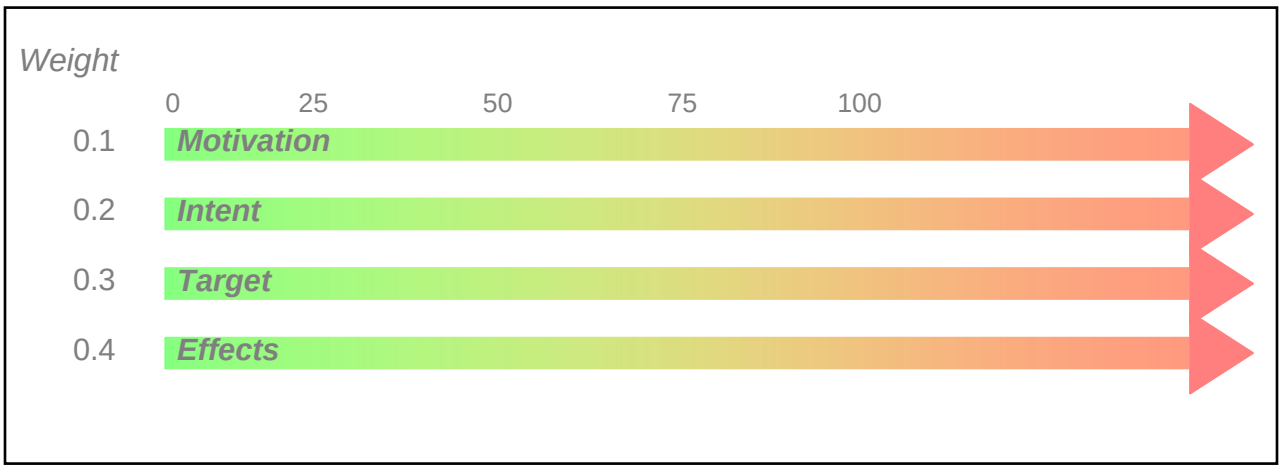


Figure 6: Combined Continuums, Notional Only

Quantification of the four critical factors is neither a linear task nor one which holds levels of subjectivity equal across each taxonomy. Though the *need* to quantify events might be subject to question, this research project reflected both the essential logic of a structured model and the dearth of such an equation.

In order to effectively quantify the four critical factors into an applicable mechanism, weighting agents are essential. To accurately capture a given event and maintain flexibility over the evolution of the mechanism, weights themselves might be subject to a multitude of interactions, depending on myriad factors. Such items include, but are not limited to, attack attribution, the timing of an attack, parallel events, political considerations and so forth. Additionally, Figure 5 is not meant to represent a viewpoint constrained to only *two* weighting systems; the volume and character of such systems was outside the range of this project, and might be best approached in a classified setting.

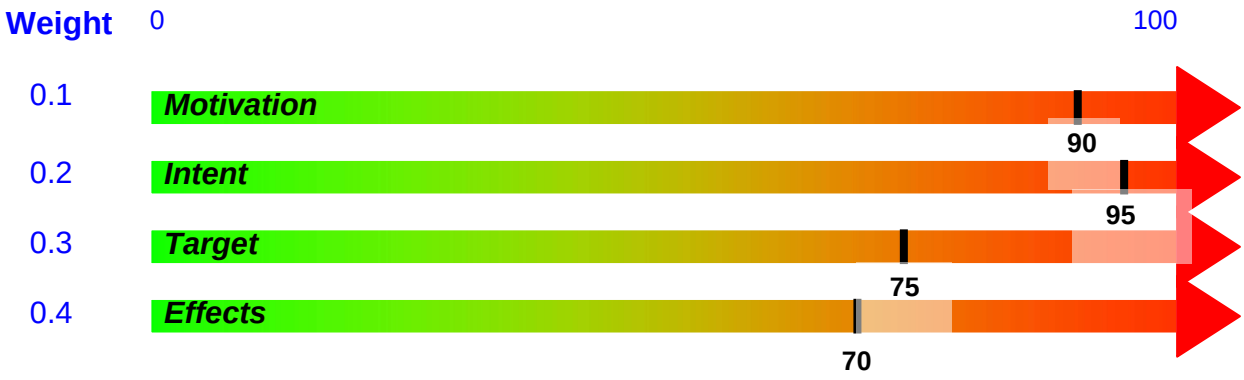
At this juncture, issues of discernment and decision-making processes are highly important. The research team deliberately avoided marking specific threshold points with labels such as “Act of War,” guided by the belief that such subjectively cannot be reflected even across the most thoroughly researched and carefully weighted scales. Indeed, the opposite is true: characterization of cyber acts will always involve levels of subjectivity, because imperfect human actors are involved. Additionally, a decision to authorize the use of force – whether via the cyber world or an asymmetric arena – obviously cannot be linked exclusively to mathematics. Therefore, assessment tools must be sharply defined and carefully calibrated over time, in order to act as *one component of many* that decision-makers at the highest levels should consider. Even in a highly technical setting, human intelligence and calculation is of utmost importance, and offers a subtlety completely missed by ones and zeroes.

Measurement

The team briefly examined the attacks on Estonia in 2007, and quantified each of the four critical factors. The table below displays the values given to each factor, the weighting of each factor, the total score for each factor, and the total "score" of the act. The following numbers are notional and only for demonstration purposes.

NOTIONAL ANALYSIS

ESTONIA INTERNET EVENTS 2007



	Score (0-100)		Weight	Subtotal
Motivation	90	x	0.1	9
Intent	95	x	0.2	19
Target	75	x	0.3	22.50
Effects	70	x	0.4	28
			Total:	**78.50**

Table 1: Quantified Assessment

Both Motivation and Intent received severe ratings based on the high degree of malice and the intent of disrupting availability of important websites. Target received a lower, but still serious, mark because of the target classification. Also, the Effects of the attack were mitigated somewhat by defenses already in place and quick action by the effected sites.

While the avoidance of certain labels, such as “act of war” was deliberate; a “tiered” notion built on threshold “scores” blanketed the research. Assuming a bounded “0” on scores for a completely benign act, a conceptual score of “100” for an extremely hostile act is not necessarily bounded – limiting such a high-end threshold is premature in an age where technology advances overnight. This notional idea is an example of what may “trigger” certain decision-making parameters, for example, a certain score might alert a given level of national security or private network managers, while a higher score might result in alerts to higher officials. Importantly, however, this example is meant as one piece of a much larger frame – as a single tool among many in an alert structure.

Further Characterization

Actor

This research concluded that the actor component, though critical to determining the appropriate response to an act, should not be included in the characterization of an act. This is due to the fact that the actor is essential when determining issues of response, but not of initial characterization. Generally, there are three categories of actors: individuals, groups, and states. Adversaries in each of these categories pose a threat to the United States, and each category may be further sub-divided into smaller groups based on the motivation of the actor. The response to

the action must take into consideration the actor, because an actor with no state affiliation may need to be approached from a legal standpoint, whereas an actor with state support may be approached through political, diplomatic or even military channels. The level of state support an actor receives assists in determining what type of response, if any, is appropriate.

Individual cyber attackers can be segmented into recreational hackers, criminals, and political or religious activists. Recreational hackers execute cyber acts for personal enjoyment and range in technical expertise from novice to proficient. Most novice hackers obtain point-and-click hacking tools and programs from hacking websites and blindly fire such tools at websites with little or no understanding of how those tools work. Generally, the effects of these endeavors by novice hackers are insignificant and are easily deflected by any significant target.

The Internet has made it possible to rapidly disseminate programs that exploit vulnerabilities in systems making it trivial for a real attacker to write a new program, exploiting a high priority target such as a component of the infrastructure, and put it on a hacking website for others to execute. Suddenly, novice hackers become the vehicle used to deliver a dangerous attack, while the author of the exploit sits and watches at a safe distance. For some individuals, hacking is a form of intellectual exercise. They often hack into a system to prove that they can, without ulterior motives. Unfortunately, once an intrusion has been made, the integrity of that system cannot be trusted. Other individual actors perform attacks for personal gain, often monetary. These individuals are essentially mercenaries, selling their talents to anyone with the money to purchase them. Individuals in this category are either very skilled, or have a higher level of access to the target, such as an insider.

Individual attackers tend to be limited by two factors: resources and aversion to risk.[184] The primary resource individual adversaries lack is funding. They can only spend what they earn from personal employment, criminal or not, and are thus restricted in the tools they can purchase. They are also the sole bearer of any legal retribution, should their actions be discovered.

The barriers that may deter an individual from carrying out an attack are a considerably smaller concern for adversarial groups. While individual attackers are generally limited by a lack of resources or risk aversion, adversarial groups tend to possess greater resources and are emboldened by their size. These groups may lack the technical expertise to design and carry out an attack, but they can purchase it.[185] Along with that purchasing power comes the ability to diversify goals: instead of a single motivation, such as profit, groups can work to carry out multiple plans of action. A few notable advesary types include organized crime organizations, terrorist networks and rogue or developing nations.

Organized crime groups have existed for centuries, using illegal gambling rings, narcotics trafficking and a host of other methods to generate profit. These organizations are increasingly using the cyber domain to carry out their crimes; both via buying resources to achieve their goals and paying talented hackers handsomely to create profitable exploits.[186] Organized crime groups also buy or create bots to carry out many of their nefarious actions such as spamming, phishing and extortion.[187] [188] These groups will often pursue riskier than an individual would, because the structure of these organizations protects those in power.

---

[184] Schneier, Bruce. Secrets and Lies: Digital Security in a Networked World. New York: John Wiley and Sons, 2000.
[185] Ibid.
[186] Murtagn, Mark. "The New Hackers on The Block." November 11,2005. http://www.biosmagazine.co.uk/op.php?id=314
[187] Lewis, James. "Cyber Attacks Explained." Center for Strategic and International Studies. 15 June 2007.
[188] Sending spam and phishing are two types of actions that can disrupt networks and frequently used by cyber actors. "Spamming" might be compared to sending junk mail, while "phishing" refers to various methods by which actors can attempt to gain unauthorized information. An example of phishing might be an actor falsely representing

Terrorist groups, such as al Qaeda and Hamas, have traditionally used low-tech methods of inflicting terror on states or ethnicities they oppose. Since the early 2000's, however, the cyber domain has been used in an ever-increasing manner by terrorist groups for communication, planning, and recruitment purposes. In 2006, the DHS warned that al Qaeda may be planning an attack on United States financial institutions.[189] While the resources examined during this project suggrest that such an attack has not materialized to date, the danger of a terrorist group launching a cyber attack is still quite real. These groups are not concerned about the risks associated with carrying out an attack and are willing to pursue any means to obtain their objective of fear and panic.

Rogue or developing nations also pose a serious threat to U.S. government networks. Some possess a wealth of money and other resources, and may have the ability to fund and execute large-scale cyber campaigns in order to obtain their objectives. In the same vein, however, developing regions realize the economic realities of world stability, and that malicious actions may undermine their own ability to grow self-sustaining capacity.

Distinctions between these three examples are sometimes blurred and can render complete identification of a cyber actor difficult. Some cyber actors are subsets of states or ideals (patriotism), and may be acting alone or in concert, making characterization doubly trying. For instance, an individual may act out of his/her own interests, but may utilize resources of the group or state to which he belongs. In such cases, it may be insufficient to simply categorize actors under a specific umbrella; it may be necessary to determine the degree of state sponsorship given to the actor.

---

themselves on the phone or via email in an attempt to prompt the receiver to respond with legitimate information (bank account numbers, passwords, etc.).

[189] "US warns of possible financial cyber attack" MSNBC, 30 November 2006. <http://www.msnbc.msn.com/id/15975889/>.

Actor Typologies

Actors fall into three basic types and four sub-genres, based on the level of state sponsorship they receive, and not all sub-genres are exclusive. For example, an individual's state support can span from none to actually funded, while a state actor is unlikely to be without official affiliation.

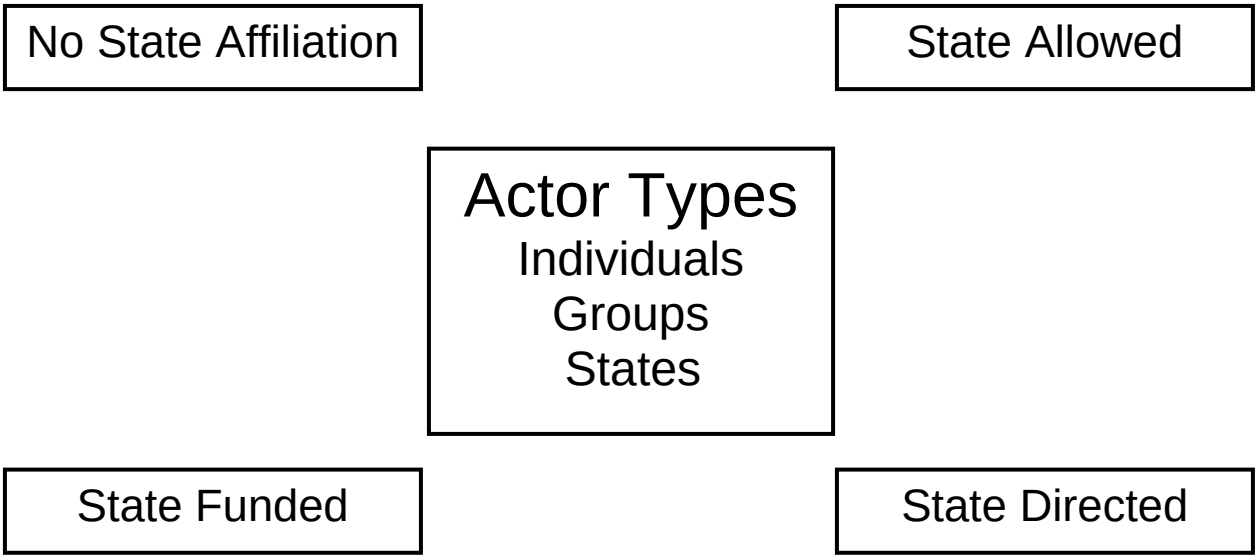


Figure 7: Actor Typologies

State sponsorship is important in determining the response a hostile cyber act may warrant. If no state affiliation can be attributed to an act, responses to the act would likely be restricted, depending on the severity of the attack outcome. For example, a single actor defacing another individual's website may face no punishment, while a foreign actor who successfully infiltrates the defense computer network of another country may be arrested. However, the effectiveness of legal response can be diminished if the country the attack originated from does not have laws against cyber attacks, or if that country refuses to cooperate with the United States

in extradition of the attacker. For this reason, many lone attackers or groups who choose to undertake high-risk attacks will launch their attacks from countries they know will harbor them.

Validating some level of direct state sponsorship for an act, such as state funding or state direction, opens up more options for response to a cyber act. These responses range from political and diplomatic responses to kinetic responses based on the severity of the act. However, proving state sponsorship is very difficult. Since states are ordinarily risk adverse, attacks sponsored by states are very well masked and difficult to trace.

Attribution

At the very heart of defining a proper response to an act is attribution. Attribution is "the ability to tie an act to an actor."[190] Without correct attribution, responses to an act are necessarily limited. Without appropriate responses to cyber acts, deterrence in the cyber domain becomes nearly impossible. Correctly attributing an act to an actor would make confirmation of motivation and intent exponentially less difficult.

Attribution of an act relies on the assumption that some characteristic or combination of characteristics uniquely identifies the object of attribution. For example, the VIN (Vehicle Identification Number) on an automobile uniquely identifies that vehicle. In the cyber domain adversaries will usually seek to disguise their identity through a number of techniques.

There are three key elements of attribution in the cyber domain: precision, accuracy and security. Precision is a measure of the exactness of the attribution. In some applications, attributing an event to a region may be enough to respond to the event. In other applications,

[190] Goodman, Seymour E. and Herbert S. Lin, Eds. "Toward a Safer and More Secure Cyberspace." National Research Council and National Academy of of Engineering, Committee on Improving Cybersecurity Research in the United States, Computer Science and Telecommunications Board, Division on Engineering and Physical Sciences. (2007), p.113.

attribution to an exact person or machine may be required. Accuracy is a measure of the quality of attribution, such as a probability that the attribution is correct. This measure is critical to the burden of proof placed on the attribution. Security of attribution is the inability to break association between action and actor. When the security of an attribution fails, impersonation or spoofing[191] can readily occur.

In the cyber realm, attribution is generally divided into four levels, each successively identifying a more exact representation of the actor.[192] The first level is attribution of the act to the attacking machines.[193] Attributing the act to the attacking machines is useful for short term deflection and defending against the attack. However, this first level of attribution offers little help in responding offensively to the act. This level is typically the starting point for all other levels of attribution.

The second level of attribution is attributing the act to the controlling machines. In order to mask the identity of the attacker, sophisticated cyber attacks will use a machine compromised by the attacker to launch the attack. Attribution of a hostile act to the primary controlling machine(s) is beneficial for the long term defense against attacks issuing from those machines. Additionally, attribution of the hostile act to the controlling machines will aid later levels of attribution. This level of attribution could allow offensive responses against the command machines, but may not necessarily justify responses pursued through political or legal channels, as the human actor is not known.

[191] "Spoofing" denotes the successful impersonation of a legitimate actor in the cyber sphere: for example, an actor who phishes for bank account information and then has ongoing contact with a responding target would have successfully "spoofed" their own identity as a bank representative to successfully "phish" the target.
[192] Denning, Dorothy. "Cyber Attack Attribution: Issues and Challenges" Powerpoint, Center for Terrorism and and Irregular Warfare, Naval Postgraduate School, March 2005.
[193] Ibid.

The third level of attribution is attributing the act to the humans mounting the attack. This is the first level of attribution that yields itself to responses through legal and diplomatic channels. However, this level of attribution cannot be ensured by technical attribution alone. It requires a combination of technical and other intelligence approaches.

The fourth level of attribution is attributing the act to the organization sponsoring the act. Similarly, this level of attribution cannot be determined through technical attribution methods alone. There is also a question of when a given cyber act may be attributed to a nation-state. Generally, states are not responsible for the conduct of private parties,[194] but states are responsible for the conduct of all divisions and all levels of government.[195] Similarly, if an entity, though not a state organ, is empowered by law to exercise government power, that entity's acts are considered state acts.[196] Even if a state organ, person or entity exceeds its authority or acts contrary to government instruction, the resulting act is an act of state.[197] Additionally, state acts also include acts perpetrated by insurgent groups or war lords who exercise governmental authority in absence or default of the official authority,[198] and acts by insurrectional movements which later become the new government.[199]

In regard to state sponsorship of a person or group, Article 8 of the International Law Commission's Non-binding Draft Articles on the Responsibility of States for Internally Wrongful Acts declares that an act is attributable to the state if a person or group is carrying out instructions or directions of state.[200] According to the International law Commission, the group

[194] Denning, Dorothy. "Cyber Attack Attribution: Issues and Challenges" Powerpoint, Center for Terrorism and and Irregular Warfare, Naval Postgraduate School, March 2005.
[195] Ibid
[196] Ibid
[197] Ibid
[198] Ibid
[199] Ibid
[200] Ibid

or person must be acting on the "instruction of" or "direction and control of" the State.[201] The Commission's definition corresponds to the "effective control" test expressed by the ICJ in US *v.* Nicaragua, which required that a state must direct the acts and control the group.[202] However, in another notable international law case, The Prosecutor *v.* Dusko Tadic, the International Criminal Tribunal for Former Yugoslavia applied a different, less-stringent standard, only requiring that the group as a whole be under "overall control" of the state.[203]

Attribution Techniques

Many different techniques are employed in the attempt to attribute an act to an actor. The techniques discussed below are some of the current methods, which have demonstrated varied success. One common method of attribution is storing logs at the routers and running traceback[204] queries against those logs.[205] [206]For this to be effective, the routers must log data about every message that passes through it. The data stored may be a piece of the message or a hash[207] of the message to reduce storage space required, but either way this method will cause performance overhead costs directly related to the size of the system implementing it. These logs are then queried to determine which routers the attack passed through. One of the advantages of this method is that it provides forensic evidence that can be used to investigate the attack at a

[201] Ibid
[202]Nicaragua *v.* United States (Military and Paramilitary Activities in and Against Nicaragua), 1986 ICJ 14.
[203] Prosecutor *v.* Dusko Tadic, IT-94-1-A, International Criminal Tribunal for the Former Yugoslavia, Appeals Chamber, 38:1518 (1999). <http://www.asil.org/insights/2006/08/insights060824.html>
[204] A general term used to describe methods by which computer logs or events are traced.
[205] Wheeler, David A. (2003) "Techniques for Cyber Attack Attribution." Institute for Defense Analysis, Paper P-3792, October 2003, p. 16.
[206] A computer log is essentially a diary or recording of events that occur on a system.
[207] A "hash" is a small set of data which represents the original, larger data set and is used to ensure secure communications across a network and reduce space usage.

later date. However, these routers and their recording systems must be in place before the attack occurs, and must be secured to prevent the adversary from tampering with the logs.

Input debugging is another common method of attributing an attack. In this approach, upstream routers (one step closer to the attacker) are given a pattern and asked to report if that pattern passes through them again.[208] By this process the defender can step back one by one through the routers the attack is progressing through until the source is found. One downside of this method is that it can only be performed if an attack is currently happening and requires that packets[209] matching the pattern continue to be sent from the source until it can be identified. Also, this method generally only allows for attribution to the attacking machine because the controlling machines will not usually send the same pattern to the controlling machine.

A third method of attribution is to modify the messages transmitted back to the attacker in a way recognizable to the defender but not to the adversary, usually by appending some characters to the stream.[210] While this approach eliminates the need to store data about the attack, it will increase bandwidth and therefore reduce performance of the network. Also, this method may break many authentication mechanisms which detect changes made in the message. This method can attribute only to the level that the messages are transmitted, and can be foiled if the adversary encrypts the message at any point.

Another avenue for performing attribution is termed a "hack back." This method assumes that the defender can follow the trail of information back to the attacking systems and exploit some vulnerability in them, possibly the vulnerability the attacker used.[211] This hack back is then repeated back up the chain until the controlling system is found. This method, however, brings

---

[208] Ibid.
[209] A formatted block of data used to transmit information; similar to a byte but more versatile.
[210] Wheeler, David A. (2003) "Techniques for Cyber Attack Attribution." Institute for Defense Analysis, Paper P-3792, October 2003, p. 16.
[211] Ibid.

up many questions about legality, especially when the hack back must attack systems in foreign countries. Additionally, manually hacking back along the path is slow and the adversary may be gone by the time it is completed. While automated hack backs are much quicker, they have the potential to damage the intermediate systems. One advantage of this approach is that level two attribution can be obtained.

Another method for attributing an act is to use "web bugs" such as beacons, cookies or LoJack™ [212] programs to report where the data is going.[213] These methods have the advantage of allowing for level two attribution and may be able to be used as evidence in a court of law. However, if the adversary knows how these methods are employed, they can easily foil them.

The final method of attribution is to use forward deployed intrusion detection systems. These systems look for known exploits and traffic anomalies and are primarily used to defend a system against attack. These systems are helpful in combating DOS attacks but can be subverted by the attacker if they are not properly secured.

Each of these methods has inherent strengths and weaknessess, and this researh shows that sole reliance on any one method would be ill-advised. Therefore, it is prudent to establish and utilize a combination of methods throughout any system where attribution is deemed important. By doing so, there will not exist the possibility of a single point-of-failure in the attribution mechanisms of the system.

[212] A "web bug" is also known as a "web beacon," and is used in concert with cookies – traffic markers usually downloaded automatically upon web site visitation -- to monitor a user's behavior. LoJack™, familiar to the general public as a system for tracking stolen vehicles, is also available for computers and laptops via ISP source tracking of a user's IP address.

[213] Wheeler, David A. (2003) "Techniques for Cyber Attack Attribution." Institute for Defense Analysis, Paper P-3792, October 2003, p. 16.

Framework Application

The 2007 cyber attack on Estonia demonstrated that the time for cyber policy discussions absent action has passed. As the world's primary defender and leader of global interests, the United States government has reached the point of criticality across cyber decision-making platforms; President George W. Bush's Homeland and National Security Presidential Directives 23 and 54, issued on January 8, 2008, speak to such urgency.[214] The recommendations encompassed in this report span a wide audit of both peer-reviewed literature and media reports; project interviews were also held throughout the Washington, D.C. area and with top officials nationwide via teleconference. The vast majority of interactions held a common thread: neither indecision nor incrementalism within the cyber policymaking spectrum is an option.

The framework presented in this paper is a straightforward representation of a complicated series of factors, in an attempt to format a degree of measurement that can be used in a proactive manner. While it is true that the framework cannot be used until a cyber act has occurred, or is realized, the baseline idea could be applied at the first sign of network traffic anomalies, assuming thorough testing and case study analysis. A real-time tracking process, then, might work to predict a cyber action based on past patterns, while its overall final assessment might be used to plan an appropriate response to the action. Overall, while parts of the framework quantification may be bounded, the framework itself is unbounded, and could theoretically be used both before, during and after a cyber acting occurs.

[214] National Security Presidential Directives of the George W. Bush Administration. Intelligence Resource Program, Federation of American Scientists, Retrieved March of 2008. http://www.fas.org/irp/offdocs/nspd/index.html

Additionally, the standard use of an agreed-upon framework need not constrain customized reactions to it; should such a universal measurement be utilized by both a government agency and a private corporation, for example, different reactions would obviously result from a cyber hostile action. From this viewpoint, the framework is both user-friendly and flexible, and might be more welcomed by private sector interests.

Items for Immediate Implementation

Formulating a universal framework for cyber actions will necessarily call into question operational definitions for such a framework. The importance of agreed-upon language in the cyber realm cannot be overstated; terminology, such as that encompassed across a cyber continuum, is key to both assessing an incident and determining a response.

That a paradigm would also necessitate standardized incident evaluation criteria and reporting procedures is obvious. According to software experts,[215] no conclusive "clearinghouse" for incident reporting has been established, and the multitude of "CERTs" beyond US-CERT and Carnegie Mellon University's CERT® has caused confusion in both the public and private sectors. One military official[216] advised that when issues arise, no one is sure "which 'CERT' to go to," while a software company representative echoed the same sentiment.[217]

Given the wide overlap across government and commercial entities, and corresponding interests, a co-sanctioned construct with uniform terms and reporting procedures would serve to elucidate a true pictorial of the nation's cyber security status. Without a complete depiction, network status reports will remain scattered and, therefore, of questionable value. On an

[215] Personal interview with software experts. Washington, D.C. 18 March 2007.
[216] Personal interview with military cyber officials at the Pentagon. Washington, D.C. 17 March 2008.
[217] Personal interview with software experts. Washington, D.C. 18 March 2007.

operational basis, the need for rules of engagement across both armed services and government entities is also priority. However policymakers opt to define cyber "attacks," numerous volumes of such actions occur daily across private and classified networks. Both military and private actors zeroed in on the lack of operational procedures, and one expert[218] advised that a framework similar to HIPAA (US Department of Health, Health Insurance Portability and Accountability Act)[219] or Sarbanes-Oxley[220] might best serve the nation's interests.

The initial steps to creating operational guidelines which enhance the cyber security of critical infrastructure are encompassed in the Federal Energy Regulatory Commission (FERC). Recently, FERC has approved reliability standards which advance the cyber security of our nation's bulk power system, by establishing policies, plans and procedures to defend electronic access to their control systems. These are important steps to safeguarding our nation's critical infrastructure, and the FERC example might also act as a model across other industries.

Domestic Policy Issues

The large volume of cyber security institutions using the "CERT" moniker clearly impede correct, and possibly widespread, utilization of the US-CERT initiative from top management levels; such uncertainty undermines the very purpose of the Computer Emergency Readiness Team. Additionally, though the CWIN system is emplaced for emergency use, its return on investment, according to cyber professionals familiar with the program, may be

[218] Personal interview: private industry cyber expert. Washington, D.C. 17 March 2008.
[219] Enacted by Congress in 1996, HIPAA requries national standards for electronic health care records and transactions, among other items. See the United States Department of Health and Human Services. http://www.hhs.gov/ocr/hipaa/
[220] Congress passed the Sarbanes-Oxley Act, known as SOX, in 1992 in the wake of acounting scandals, most notably surrounding the Enron Corporation. SOX is mandatory legislation requiring financial process compliance by all US-listed corporations, regardless of size. See resources from The University of Cincinnati: <http://www.law.uc.edu/CCL/SOact/toc.html>

questionable. A review of both US-CERT and CWIN for issues of both relevance and efficacy may serve to elucidate current national security needs.

In addition, there is a need for clarifying and instituting domestic legislation that speaks directly to cyber issues. In the United States, a number of federal crimes exist for prosecuting cyber malfeasance, including mail and wire fraud and statutes prohibiting the issuance of threats and solicitations of violent crimes.[221] The USA Patriot Act of 2001 (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act) authorized law enforcement and intelligence agencies to expand monitoring of Internet traffic in pursuit of terrorists.[222] Additionally, the 2002 Federal Information Security Management Act (FISMA) required the head of each federal agency to provide information security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification or destruction of information systems.[223] Even with such laws in place, the lack of agreed-upon legal terminologies for cyberspace is a barrier, and the lack of a national cyberspace doctrine works to impede progress made through such legislative efforts.

While it is true that the law, inherently, must "ripen" before it can mature, technically based statutes that speak to existing instances of crime and terrorism can assist law enforcement in both investigatory and prosecutory duties. As the networks further pervade American life, human nature will undoubtedly find new ways to exploit both technical vulnerabilities and social engineering opportunities to an extent likely unfathomable today. Though the law is not

[221] Ganeles, Cheri. "Technological Advancements and the Evolution of Terrorism." International Law Students Association Journal of International and Comparative Law, 8:167, Spring 2002.
[222] Ibid.
[223] United States. Government Accountability Office. 2007. Information Technology: Numerous Federal Networks Used to Support Homeland Security Need to Be Better Coordinated with Key State and Local Information-Sharing Initiatives. April 2007.

traditionally proactive, in order to mitigate critical infrastructure damage, those who would misuse or abuse critical national infrastructure must be held accountable.

Future National Directions

Industry experts and academic scholars alike insist that the development of public-private partnerships is crucial to undertake the issue of cyber security. With about 85 percent of the nation's critical infrastructure in the hands of the private sector, the need for cooperation among both sectors is obvious.[224] The framework for such may already be emplaced, however; according to experts, government security structures are already adequate, and the private sector maintains resources that are not being fully utilized.[225] Instead of building additional public-private entities, experts argue for the enhancement and improvement of existing relationships.[226] Indeed, the growth of ISACs and other cyber security groups over the last decade may be acting to prohibit efficacy; the quality and relevance of existing dialogue, not the quantity of such conversations, is therefore urged.[227]

Additionally, the research framework in this paper does not address a vital area of concern: the pairing of a cyber attack with a physical attack.[228] Experts assert that an attack on the electric power grid could take out power for up to 6 months or even just enough time to accomplish the attackers' end result.[229] National infrastructures such as the electric power grid need to be better protected from possible intrusions which, alone or along with a physical attack,

[224] United States. Government Accountability Office. 2006. Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by by Sectors' Characteristics. October 2006.
[225] Personal interview: private industry cyber expert. Washington, D.C: March 17, 2008.
[226] Cyber Roundtable discussion, Washington D.C., May 14, 2008.
[227] Ibid.
[228] Ibid.
[229] Cyberwar!" Frontline PBS, 24 April 2003.

could cause severe harm and damage.[230] While such a characterization was beyond the scope of this project, further development of any qualitiative metric may be considered lacking without this possibility. Importantly, any overall model for characterization would almost certainly require a mixed methodology to capture both numeric and subjective qualities of a cyber action.[231]

International Purview

In regards to foreign policy concerning the cyber realm, one may look to the only international treaty of its kind, the Council of Europe Convention on Cybercrime. The Convention is the first to address the issues of cyber security and cyber crime from an international perspective. The United States, though not a voting member to the Council of Europe, is party to the Convention. Although the Convention is indeed a very good start to addressing hostile acts in cyberspace, one must note that the Convention was established only to address cyber crime. This includes child exploitation and cyber fraud, but not issues of cyber conflict and cyber warfare between nation states.

NATO has commenced efforts to address these issues in cyberspace by outlining the foundations of an international treaty and establishing the Cyber Defense Management Authority – which will be the central structure managing developing issues and new tasks that accompany cyber security at the international level.[232] While the Cyber Defense policy accentuates the need for the assistance of Allied members in the occasion of a cyber attack, it will fall exclusively under Article 4 of the North Atlantic treaty. Article 4 states that members, "will consult together

[230] Ibid.
[231] Cyber Roundtable discussion, Washington D.C., May 14, 2008.
[232] North Atlantic Treaty Organization. Bucharest Summit Declaration. 3 April 2008

whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened." It is important to note that this statement sidesteps the issue of whether fellow member countries will be compelled to come to the aid of a member country under cyber attack, which is outlined in Article 5 of the treaty.[233]

International agreements are a critical component in cyber security. The Council of Europe's Convention on Cyber Crime and NATO's inaugural strides with their Cyber Defense policy are valuable endeavors. However, they are still not enough to embark upon the issues of cyber crime, conflict, and warfare. In order to effectively and entirely address these international issues, more global agreements, similar to the Convention on Cyber Crime, need to be encouraged and established. Further global agreements must include all aspects of the cyber realm, including conflict and warfare. Additionally, to aid in the advancement of global agreements, international laws concerning the cyber realm should be clarified and instituted.

Further Research

Throughout the course of this research, issues of importance have surfaced that, while beyond the scope of the given project, hold direct consequence for cyber security over short and long-term platforms. National security managers must look far beyond mere network occurrences and user traffic patterns to ensure a sustainable level of structural integrity.

First, the origin of computer components and the location in which they are assembled is of grave concern. Such an issue goes beyond geography, as trusted and verifiable partners can exist anywhere in the world, to the actual processes and personnel used to build network equipment in a given plant. Large quantities of desktops, laptops, and their associated peripherals

[233] NATO Agrees Common Approach to Cyber Defense." EurActiv.com. 4 April 2008. April 2008 < http://www.euractiv.com/en/infosociety/nato-agrees-common-approach-cyber-defence/article-171377

are manufactured outside of the United States, and both commercial and private consumer purchases may represent a significant risk for manipulation in this area. In the private and small business arenas, it is unlikely that desktop central processing units or laptop hard drives will be opened and examined by the purchaser, and more unlikely that such a buyer will replace their own memory or perform custom upgrades. For military acquisition managers, the threat is even higher. A strong investigatory review into this issue, including the possibility of a domestic manufacturing construct, is highly recommended.

Secondly, while private-public cooperation is key to securing domestic infrastructure – a point widely discussed throughout the cyber security literature and related congressional testimony – the private sector does not operate under an altruistic guise. To encourage cyber security investment by businesses, a financial incentive is necessary, and might be gleaned through liability protection or tax credits issued upon the integration of certain standards or security purchases.

Finally, public computer networks have matured over the past decade, and according to experts, $2.5 trillion moves across the world electronically on a daily basis.[234] The advent of digital signatures and secure networks was perhaps inevitable; the wide availability of commercial encryption software speaks to market demand. Logic holds that an encrypted platform would eventually be integrated across the public Internet, though this has not yet occurred. The notion of publicly encrypted networks is not new; this research project has spoken to the need for a renewed discussion in this area.

Conclusion

[234] Personal interview: private industry cyber expert. Washington, D.C. 17 March 2008.

A common thread ran through this project's consultations with cyber experts, researchers and practitioners: the need for immediate action and attention across the highest levels of government and industry. From executive suites in downtown Washington, D.C. to the corridors of the Pentagon, similar sentiments were echoed, and with them, interesting ideas on how the GISC research team – and further, official policymakers – might proceed. Though the "comfort zone" of theoretical cyber realms was reflected throughout discussions – "How can an 'attack' be delineated from an 'act of war'" – such debates do not move national security priorities forward. Not unlike the national unity seen post 9/11, a compromised consensus must be reached across the public and private sector if the United States is going to take network security seriously. In the cyber world, policy incrementalism is deadly.

There is no doubt that the private industry has vast resources,[235] and most actors acknowledged that multiple teams in multiple areas were working diligently on these problems. However total that effort, the piecemeal reality of current nationwide implementation rang clear throughout the project; sources conveyed a sense of dislocation about their own attempts to cross public-private boundaries. A lack of confidence was reported in particular areas of federal control, and comments surrouding cyber responsibility was mixed. Some industry leaders iterated their concern, and corresponding activities, regarding cyber security; others took a nonchalant pose, positing their own immunity, and still others spoke of a "patriotic" duty to assist the public sector in reporting suspicious activity across their networks. Most sources, however, considered the a universally agreed upon framework for characterizing cyber acts – or at the very least, a consensus-type framework – a necessary starting point.

Commencing from the work of Thomas Wingfield and Michael Schmitt, the research team spent many hours reading peer-review literature on measurement techniques. After the

[235] Personal interview: private industry cyber expert. Washington, D.C. 17 March 2008.

outreach and initial interview phase, team members roundtabled measurement criteria, and – using backgrounds in Law, Computer Science, Psychology, Information Assurance, Public Administration, Political Science and Management Information Systems – approached the measurement problem with an eye toward an agile model to serve as a baseline. After speaking further with field experts, certain ideas were discarded and new considerations – such as cryptography and hardware integrity – were drawn into the circle of importance. Additionally, the team had the opportunity to brief the Air Force Science Advisory Board prior to project completion, and insight garnered in that forum enhanced preliminary thought on the subject.

Primarily, the final result reflects the original research question: How should the United States characterize acts in cyberspace? While the numbers and weighting systems are nascent, the idea is fresh: a uniform framework that could be built over time, with the understanding of evolutionary and agency-specific input from the onset. The entire project screams for uniformity; the one problem that overshadows all, from language to incident reporting, to investment and even basic comprehension of the problem, which is often intangible. Cyberspace has matured at an exceptional pace, and requires a mature and carefully formatted lens through which to view it. This is especially true in the military world, today so heavily dependent on electronic cobwebs, which literally equates to life and death – very tangible issues.

A utilization of the type of model presented here in both private and public industry may lead to better utilization of programs such as US-CERT, and obviously includes the CWIN component as a tool for pattern recognition reporting. If both the public and private arenas are using the same basic roadmap, communication between the two would occur on a more natural basis, leading to a higher level of cooperation, understanding, and bilateral information sharing.

Additionally, legislatures would hear from constituencies across the board and be empowered to better address statutory and budget needs. Such a window obviously encourages broad-based conversations among American allies, and through such consortiums, global dialogue and expanded prosecution of hostile cyber actors based throughout the world. The “new world” is indeed small, and speaking the same “language” would remove many of the cooperative and financial barriers seen today.

Finally, no cyber act characterization framework can be fully trusted if the hardware on which information is gathered is compromised. A review of domestic manufacturing dependencies, inline with domestic investment in private sector security, allows burning the national security candle at both ends, all the while avoiding a fire. From this vantage point, public encryption is a natural consideration; past controversies surrounding law enforcement “switching” access to such systems is dulled by the wide availability of Secure Sockets Layer (SSL) platforms consumers are today very familiar with.

Information sharing may be the buzzword of the millennium, but it is vital – not optional – in the cyber world. As military and business leaders consistently point out, the United States is constantly behind in math, engineering, science and the cyber realm itself. Computer networking has grown up; it is time for policymakers to follow suit.

Works Cited

Abbot, Marrianne & Jill Egeth. “Intentions, Motivations, and Violent Non-State Actors.” Powerpoint presentation, Military Operations and Research Society, MITRE Corporation. 5 February 2008.

Air Force Cyber Command Strategic Vision. Comments by Major General William T. Lord. (n.d.).

Alexander, Yonah, and Michael Swetnam. Report to the President’s Commission on Critical Infrastructure Protection: Cyber Terrorism and Information Warfare. Vol. 3. Dobbs Ferry, New York: Oceana Publications, 1999.

Allen, Patrick D and Chris Demchak. “The Palestinian-Israeli Cyberwar.” Military Review. March-April 2003.

Anderson, James P. Computer Security Technology Planning Study, Volume II. USAF Electronic SystemsDivision, Command and Management Systems, 1972.

Antolin-Jenkins, Vida. “Defining the parameters of cyberwar operations: looking for law in all the wrong places.” Naval Law Review, 51:132. (2005).

Archick, Kristin. “Cybercrime: The Council of Europe Convention.” Congressional Research Service Report for Congress. 28 September 2006.

Arquilla, John. 2008. E-mail to Stephanie D. Silva, July 10, 2008.

Binnendijk, Hans, ed. Transforming America’s Military. National Defense University Center for Technology and National Security Policy, National Defense University Press, 2002.

Brenner, Susan W. “At Light Speed: Attribution and Response to Cyber Crime/Terrorism/Warfare.” The Journal of Criminal Law and Criminology , 97:2 (2007).

Cabana, Nonie. ”Cyber Attack Response: The Military in a Support Role.” Air & Space Power Journal, April 4 2008. <http://www.airpower.maxwell.af.mil/airchronicles/cc/cabana.html>.

Cornell University Law School, US Code Collection, Title 18.

Council of Europe. “About the Council of Europe.” Retrieved from the world wide web March 2008. <http://www.coe.int>

Council of Europe. Convention on Cyber Crime. Explanatory Report. 8 November 2001. <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>

Cyber Roundtable discussion, Washington D.C., May 14, 2008.

"CyberWar!" Frontline, PBS, 24 April 2003.

Denning, Dorothy. "Cyber Attack Attribution: Issues and Challenges" Powerpoint, Center for Terrorism and and Irregular Warfare, Naval Postgraduate School, March 2005.

Department of Homeland Security. "Leadership." Retrieved from the world wide web March 2008. <http://www.dhs.gov/xabout/structure/gc_1157655281546.shtm?>

Department of Homeland Security. Retrieved from the world wide web March 2008. http://www.dhs.gov

"Eligible Receiver." Defense Technical Information Center, powerpoint. Accessed world wide web April 2008. <www.dtic.mil/doctrine/training/wjtsc07_2wg_exsynch_er.ppt>

Ellis, Bryan W. "The International Legal Implications and Limitations of Information Warfare: What Are Our Options?" US Army War College Strategy Research Project, 10 April 2001.

Federation of American Scientists. "National Security Presidential Directives, George W. Bush Administation." May 5, 2008.

Federation of American Scientists, Retrieved March of 2008. http://www.fas.org/irp/offdocs/nspd/index.html

"FERC approves new reliability standards for cyber security." News Release, FERC.gov, 17 January 2008.

Fidler, David P. "The International Legal Implications of 'Non-Lethal Weapons.'" Michigan Journal of International Law, 21:51 (1999).

Fine, Matt. Personal interview. Washington, D.C.: 17 March 2008.

Franklin, Jason, et al. "An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants." Conference on Computer and Communications Security, Alexandria, Virginia October 29 – November 2, 2007.

Ganeles, Cheri. "Technological Advancements and the Evolution of Terrorism." International Law Students Association Journal of International and Comparative Law, 8:167, Spring 2002.

Garcia, Gregory. Prepared remarks by Department of Homeland Security Assistant Secretary for Cyber Security and Communications. 2007 RSA Conference in San Francisco, February 5-9, 2007.

Grant, Rebecca. “Special Report: Victory In Cyberspace." Air Force Association Special Report, October 2007.

Goodman, Seymour E. and Herbert S. Lin, Eds. “Toward a Safer and More Secure Cyberspace.” National Research Council and National Academy of of Engineering, Committee on Improving Cybersecurity Research in the United States, Computer Science and Telecommunications Board, Division on Engineering and Physical Sciences. (2007), p.113.

Hare, Forrest. Personal interview: Washington, D.C. 17 March 2008.

Heaton, J. Ricou. “Civilians at War: Reexamining the Status of Civilians Accompanying the Armed Forces.” Air Force Law Review, 57 (2005).

Hershfield, Mark. 2008. “Mandatory Reliability Standards for Critical Infrastructure Protection.” E-mail to Stephanie Silva, May 5, 2008.

HIPAA. Health Insurance Portability and Accountability Act of 1996. http://www.hhs.gov/ocr/hipaa/

“Information Assurance Technology Analysis Center: History.” (n.d.). <http://iac.dtic.mil/iatac/history.html>.Staff Instruction, 3510.01D, 21 March 2008.

Information Technology – Information Sharing and Analysis Center (IT-ISAC): “Frequently Asked Questions,” 2006. Accessed via the world wide web April 2008. https://www.it-isac.org/faq.php

IT-ISAC. 2006. <https://www.it-isac.org/aboutitisac.php>.

IT-ISAC interview, Washington, D.C. 17 March 2008.

Jensen, Eric. “Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense.” Stanford Journal of International Law, Vol 38, pp 207-240.

Joint Chiefs of Staff. “No-notice Interoperability Exercise Program.” Chairman of the Joint Chiefs of Staff Instruction, 3510.01D, 21 March 2008.

Kearly, Timothy. “Raising the Caroline.” Wisconsin International Law Journal,17.2 (2007).

Krebs, B. 2007. “FBI Unveils Movable Feast with ‘Operation Bot Roast.” The Washington Post, June 13, 2007.

Kuehl, Daniel. Personal interview. Washington, D.C.: 17 March 2008.

Landler, Mark, and John Markoff. “Digital Fears Emerge After Data Siege in Estonia.” New York Times, 29 May 2007.

Lemos, Robert. 2005. “Cybersecurity Czar will have hard road ahead.” Security Focus, June 2, 2005.

Lewis, James. “Cyber Attacks Explained.” Center for Strategic and International Studies. 15 June 2007.

Libicki, Martin. “Ghosts in the Marchines?” US Foreign Policy Agenda, USIA Electronic Journal. 3:4 (1998).

Libicki, Martin. Personal interview. Washington, D.C.. 18 March 2008.

Litman, Jessica. “Symposium: The Internet: Law without borders in the information age.” The Wayne Law Review, 43 (1996), pp 95-98.

Lopez, C. Todd. “Fighting in cyberspace means cyber domain dominance.” Air Force Print News, 28 February 2007.

Lowry, John. “Technical Considerations in Cyber Conflict,” Journal of Cyber Conflict Studies, Vol. 1, No. 1, Arlington, VA. Cyber Conflict Studies Association, November 2005.

Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. US), 1986 I.C.J. 14

Murtagn, Mark. 2005. “The New Hackers on The Block.” Bios Magazine, November 11, 2005. http://www.biosmagazine.co.uk/op.php?id=314

National Security Presidential Directives of the George W. Bush Administration. Intelligence Resource Program, Federation of American Scientists, Retrieved March of 2008.< http://www.fas.org/irp/offdocs/nspd/index.html>

“NATO Agrees Common Approach to Cyber Defense.” EurActiv.com. 4 April 2008. <http://www.euractiv.com/en/infosociety/nato-agrees-common-approach-cyber-defence/article 17137 >

Nicaragua v. United States (Military and Paramilitary Activities in and Against Nicaragua), 1986 ICJ 14.

North Atlantic Treaty Organization. Bucharest Summit Declaration. 3 April 2008.

O’Connell, Mary Ellen. “Enforcing the Prohibition on the Use of Force: The UN’s Response to Iraq’s Invasion of Kuwait.” Southern Illinois University Law Journal, 15: 453 (1991).

Personal interview with military cyber officials at the Pentagon. Washington, D.C. 17 March 2008.

Personal interview with private industry cyber expert. Washington, D.C. 17 March 2008.

Personal interview with software experts. Washington, D.C. 18 March 2007.

Pfleeger, Charles P. and Shari Lawrence Pfleeger. Security In Computing, 3rd Edition. Upper Saddle River, NJ: Prentice Hall, 2003.

Prosecutor v. Dusko Tadic, IT-94-1-A, International Criminal Tribunal for the Former Yugoslavia, Appeals Chamber, 38:1518 (1999). <http://www.asil.org/insights/2006/08/insights060824.html>

Rochte, Russell C. Roundtable discussion, Washington D.C. 14 May 2008.

Rollins, John, and Clay Wilson. "Terrorist Capabilities for Cyberattack: Overview and Policy Issues." Congressional Research Service Report for Congress, 22 January 2007.

Sarbanes-Oxley Act of 2002. <http://www.law.uc.edu/CCL/SOact/toc.html>

Schmitt, Michael. "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework." Institute for Information Technology Applications, Research Publication 1, June 1999.

Schneier, Bruce. Secrets and Lies: Digital Security in a Networked World. New York: John Wiley and Sons, 2000.

Software Engineering Institute, Carnegie Mellon. 2008. "The CERT FAQ." <http://www.cert.org/faq/cert_faq.html>

Stanton, James R. "Cyber Security under the NERC Reliability Standards." IT Compliance Magazine, Spring 2007.

"The Computer Intrusion Section: FBI Cyber Division." Federal Bureau of Investigation booklet. Obtained March 17, 2008., J. Edgar Hoover Building, 935 Pennsylvania Avenue, NW, Washington, DC 20535-0001

Thompson, Bennie G. Letter to Secretary Michael Chertoff. 01 February 2008. One Hundred Tenth Congress, US House of Representatives, Committee on Homeland Security, Washington, D.C. 20515.

Thornburgh, Nathan. "The Invasion of the Chinese Cyberspies." Time, 29 August 2005. <http://www.time.com/time/printout/0,8816,1098961,00.html>.

UN Charter, Article 2(4). http://www.un.org/aboutun/charter/index.html.

UN Charter, Chapter VII. <http://www.un.org/aboutun/charter/index.html.>

UN Charter, Article 42. <http://www.un.org/aboutun/charter/index.html.>

UN Charter, Article 51. <http://www.un.org/aboutun/charter/index.html.>

UN Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States. <http://www.un.org/documents/ga/res/36/a36r103.htm.>

United Nations General Assembly, Definition of Aggression Resolution 3314 (XXIV). http://www.jstor.org/stable/view/2200318?seq=1.

United States. Defense Threat Reduction Agency. Terrifying Landscapes: A Study of Scientific Research Into Understanding Motivations of Non-State Actors to Acquire and/or Use Weapons of Mass Destruction by Kay Hayden, 2007.

United States. Department of Defense. "Information Operations Roadmap," October 30, 2003, p. 44.

United States. Department of Defense. Memorandum from the Office of the Secretary of Defense, definition of Cyberspace, May 12, 2008.

United States. Executive Office of the President. "Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting." OMB Memorandum for Heads of Executive Departments and Agencies from Director Joshua Bolton. August 6, 2003.

United States. Government Accountability Office. 2006. Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by by Sectors' Characteristics. October 2006.

United States. Government Accountability Office. 2007. Information Technology: Numerous Federal Networks Used to Support Homeland Security Need to Be Better Coordinated with Key State and Local Information-Sharing Initiatives. April 2007.

United States. Testimony of Delaware Senator Thomas Carper, Federal Financial Management, Government Information and International Security Subcommittee before the United States Senate Committee on Homeland Security and Government Affairs, 109th Congress. 19 July 2005.

United States. The National Strategy to Secure Cyberspace. February 2003. http://www.whitehouse.gov/pcipb/

United States. Office of Intelligence and Analysis for Homeland Security. Homeland Security Assessment. 5 June 2007.

United States. US House of Representatives. Committee on Homeland Security. Statement of Representative Bennie G. Thompson, Chairman: "The Cyber Initiative." Washington, D.C. 28 February 2008.

US-CERT. (n.d.). Retrieved from the world wide web in February 2008. <http://www.us-cert.gov/aboutus.html>

US-CERT. (n.d.). Retrieved from the world wide web in March 2008. http://www.us-cert.gov/contact.html

US-CERT. (n.d.). "Related Resources: Information Sharing and Analysis Centers." <http://www.us-cert.gov/resources.html.>

"US warns of possible financial cyber attack" MSNBC, 30 November 2006. <http://www.msnbc.msn.com/id/15975889/>.

Walker, Carolee. "US Senate Votes to Ratify Cybercrime Convention." America.gov. 7 August. 2006. March 2008 <http://www.america.gov>

Walker, Jeffrey K. "The demise of the nation-state, the dawn of new paradigm warfare, and a future for the profession of arms." Air Force Law Review, 51: (Spring 2001).

Westby, Jody. "Countering Terrorism with Cyber Security." Paper for the 36th Session World Federation of Scientists, International Seminars on Planetary Emergencies, Erice, Italy, August 18-26, 2006.

Wilson, Clay. "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress." Congressional Research Report Service for Congress, 29 January 2008.

Wilson, Clay. "Emerging Terrorist Capabilities for Cyber Conflict Against the US Homeland." Congressional Research Service, 1 November 2005.

Wilson, Clay. "Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Issues." Congressional Research Service Report for Congress, 20 March 2007.

Wheeler, David A. 2003. "Techniques for Cyber Attack Attribution." Institute for Defense Analysis, Paper P-3792, October 2003, p. 16.

About the Authors

Kyle Dobitz is an undergraduate at the University of Nebraska at Lincoln studying Computer Engineering. He is extensively involved in hurricane relief efforts along the Gulf Coast.

Brad Haas of the University of Nebraska at Omaha is an undergraduate student pursuring a double major in Computer Science and Information Assurance. He is currently assisting faculty research at the Peter Kiewitt Institute.

Michael Holtje is a Ph.D. candidate at the University of Nebraska at Lincoln and holds a J.D. and M.A. in Psychology. He was awarded the Presidential Management Fellowship in 2008 and currently resides in Washington, D.C .

Amanda Jokerst graduated magna cum laude from the University of Nebraska at Omaha with a Bachelor's of Political Science in May 2008. She will begin pursuing her J.D. at California's Southwestern Law School in the Fall of 2008.

Geoff Ochsner of the University of Nebraska at Omaha is an undergraduate pursuring a double major in Computer Science and Management of Information Systems. Geoff is a recipient of the Walter and Susan Scott Scholarship and holds a chairmanship in the Delta Chi chapter of Pi Kappa Alpha.

Stephanie D. Silva is an M.P.A. candidate at the University of Nebraska at Omaha, specializing in Public Policy. She sits on the board of the Omaha chapter of the FBI's Infragard program.